

COMPUTER LOGIC REDUNDANCY IN
NUCLEAR REACTOR SAFETY SHUTDOWN CIRCUITS

Frank R. Utsch

DUDLEY KIRKPATRICK
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA 93940

COMPUTER LOGIC REDUNDANCY IN
NUCLEAR REACTOR SAFETY SHUTDOWN CIRCUITS

Frank R. Utsch

The Pennsylvania State University

The Graduate School

Department of Nuclear Engineering

Computer Logic Redundancy in Nuclear
Reactor Safety Shutdown Circuits

A Paper in
Nuclear Engineering

by

Frank R. Utsch

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Master of Engineering

March 1976

Date of Approval:

M. A. Schultz, Professor of
Nuclear Engineering

Warren F. Witzig, Head of the
Department of Nuclear Engineering

Thesis
u8

ACKNOWLEDGMENTS

The author wishes to express his deepest appreciation and sincere thanks to Professor M. A. Schultz for his guidance, assistance and advice in the course of this paper and whose initial speculation prompted this study.

TABLE OF CONTENTS

	<u>Page</u>
ACKNOWLEDGMENTS	ii
LIST OF TABLES	iv
LIST OF FIGURES	v
I. INTRODUCTION	1
II. ANALYSIS OF BABCOCK-241 NSS SAFETY SHUTDOWN SYSTEM	5
III. BACKGROUND OF LOW LEVEL LOGIC REDUNDANCY IN COMPUTER SYSTEMS	27
IV. VARIATIONS OF BABCOCK-241 NSS SAFETY SHUTDOWN SYSTEM	35
V. NUMERICAL ANALYSIS OF MODIFIED SAFETY SHUTDOWN SYSTEMS	43
VI. SUMMARY AND CONCLUSIONS	47
BIBLIOGRAPHY	53
APPENDIX I - Failure Rate Data	56
APPENDIX II - Failure Rates Used in Analysis	59
APPENDIX III - Truth Tables	63

LIST OF TABLES

Table		Page
1	Legend for Reliability Block Diagrams	11
2	Failure Rates Used in Analysis	21
3	Unreliability of Voters and Voter-Switches with Powered Standby Channels	28
4	Selected Failure Rate Data	56

LIST OF FIGURES

<u>Figure</u>		<u>Page</u>
1	Fail-to-Danger Reliability Diagram for Babcock-241 NSS Automatic Safety Shutdown System	8
2	False Scram Reliability Diagram for Babcock-241 NSS Automatic Safety Shutdown System	17
3	Reliability Diagram Main and Secondary Power SCR's	19
4	Babcock-241 NSS Automatic Safety Shutdown System Failure Probability vs. Repair Time Interval	25
5	Life Stages of a THISS-2 Voter-Switch	32
6	Fail-to-Danger Reliability Diagram for Automatic Safety Shutdown System with three-out-of-five Voter Device	36
7	False Scram Reliability Diagram for Automatic Safety Shutdown System with three-out-of-five Voter Device	37
8	Fail-to-Danger Reliability Diagram for Automatic Safety Shutdown System with THISS-2 Voter-Switch	38
9	False Scram Reliability Diagram for Automatic Safety Shutdown System with THISS-2 Voter-Switch	39
10	Life Stages of a THISS-2 Voter-Switch with Two Undetected Failures	41
11	Automatic Safety Shutdown System Failure Probability with three-out-of-five Voter Device vs. Repair Time Interval	44
12	Automatic Safety Shutdown System Failure Probability with THISS-2 Voter-Switch vs. Repair Time Interval	45
13	False Scram Failure Probability of Automatic Safety Shutdown Systems vs. Repair Time Interval	46

LIST OF FIGURES (cont.)

<u>Figure</u>		<u>Page</u>
14	Automatic Safety Shutdown Systems Failure Probability for Overpower Accident vs. Repair Time Interval	48
15	Automatic Safety Shutdown Systems Failure Probability for Loss of Coolant Accident vs. Repair Time Interval	49
16	False Scram Failure Probability of Automatic Safety Shutdown Systems vs. Repair Time Interval	50

I. INTRODUCTION

Present day reactor safety shutdown circuits and engineered safeguard circuits are highly reliable. Yet public pressure continues to provide impetus to make them even more reliable. The present high reliability is obtained primarily through the use of on-line testing of redundant coincident circuits. Safety shutdown systems of new nuclear power plants will also employ either functional or equipment diversity in some form to further increase the reliability. These techniques have now increased the circuit reliability to the extent where further improvement in circuit reliability is masked by the limitations imposed by extrinsic common mode faults. Progress is also being made in this area as designers and architect engineers begin to employ separation criteria and standards for cabling and equipment, and become more conscious of the need to take extreme precautions to insure the independence of individual safety channels.

A new element, however, is beginning to appear in advanced safety system designs. This is the use of the computer to create alarms, setbacks or scrams from derived variables^{1,2,3,4}. Variables and functions such as power vs. flow, departure from nucleate boiling, local power density, etc. can all be calculated and used as advanced safety trips that will enable maximum core utilization. In addition, future projections of input safety variables indicate the use of possibly hundreds of in-core signals, which can be handled efficiently only by computer techniques.

The problem now arises as to the reliability of the computer. This problem can be split into two parts, hardware reliability

and software reliability. With the continual decline in prices of computer hardware over the last several years, the projections call for the use of redundant calculators or computers to again increase the reliability through the use of on-line repair. References 1 to 4 indicate designing in two-out-of-three or two-out-of-four computers to be used as simple hardware components.

The software situation is more complex in that it is most difficult to prove that the software will first be able to respond properly to every safety situation, and secondly, that the software which must be used to test the hardware provides complete and thorough tests. Considerable, if not all, software problems may be eliminated through the use of small dedicated microcomputers that perform only specific functions and receive their instructions through fixed read only memories.

To obtain high reliability for the computers and the system still calls for relatively high frequency periodic test and maintenance. Self-checking schemes are possible, but these again usually increase the required software. So it appears that some manual maintenance would be required to test and repair the computer, as well as its adjacent components in the system.

The introduction of people via the maintenance and repair process then raises again the spectre of the common mode faults. It has been indicated⁵ in a study of cause of plant outages in 1973 that operator error was the cause of 18% of all forced outages. By far the largest proportion of these errors were in some way related to a test and maintenance operation. So it appears as though worthwhile gains in availability might be possible if the high reliability of the safety

systems could be maintained by some scheme that increased the maintenance interval and lessened the dependence upon people.

An adjacent problem was faced by NASA in the development of a computer for on-board use for deep space probes. Here the mission length was to be ten years or more and obviously direct human maintenance was impossible. Initial studies were begun in 1961 that led to the ultimate development of the STAR (Self-Testing and Repairing) computer⁶. This computer was a fault tolerant design, and employed several forms of advanced redundancy, some of which were at a logic system level.

It is these advanced forms of computer logic redundancy which will be investigated in this paper for their potential use in nuclear safety circuits. Prior to this step, a reliability analysis of an advanced safety system employing conventional logic redundancy is required. This will serve as a standard for comparison purposes to determine if these advanced forms of computer logic redundancy do indeed result in substantial increases in either system reliability or availability over a system employing conventional logic redundancy.

As previously indicated, a number of vendors have begun employing the use of computers or mini-computers (calculating modules) in their advanced safety system designs to create alarms, setbacks or scrams from derived variables. In the United States, Combustion Engineering (CE) and Babcock and Wilcox (B&W) have submitted proposals^{3,4} for advanced nuclear steam supply systems to the Nuclear Regulatory Commission (NRC). Both safety system designs employ conventional two-out-of-four logic redundancy at the channel logic level. The CE design relies heavily on the use of relays in the various logic circuits in the system.

Conversely, the B&W design utilizes solid state technology in the logic circuits and in many other components as well. Thus, since the general trend appears to be in the solid state direction and the use of integrated circuits is on the increase, the B&W design was chosen as the standard against which identical safety systems employing computer logic redundancy would be compared.

II. ANALYSIS OF BABCOCK-241 NSS SAFETY SHUTDOWN SYSTEM

Babcock and Wilcox have prepared reference 4, referred to as Babcock-241 NSS, as a step towards standardization of a new nuclear steam system in accordance with the "reference system" option set forth in the AEC standardization statement of 5 March 1973. The major design features of all the safety related instrumentation and control systems are similar to those of the Washington Public Power Supply System (WPPSS) Nuclear Project No. 1 (WNP-1) Plant⁷ with a number of differences. There are two principal differences:

1. The Babcock-241 NSS utilizes a Plant Protection System (PPS) which comprises the Reactor Protection System (RPS) and the Engineered Safety Features Actuation System (ESFAS). The logic of the ESFAS has been changed from a two-out-of-three logic to a "one-out-of-two taken twice" logic.

2. The Babcock-241 NSS utilizes a computer (calculating module) to create alarms, setbacks or scrams from derived variables.

The RPS is described in section 7.2 and the RPS logic is shown in Figure 7.2-1 of reference 4. The Control Rod Drive Control System (CRDCS) trip portion of the ESFAS is described in section 7.4 and illustrated in Figure 7.7-4, also in reference 4. The reader is referred to reference 4 for a detailed discussion of the RPS and CRDCS. A brief summary is provided here.

The RPS is a redundant four-channel system in which the four protection channels are brought together in identical two-out-of-four logic networks in the reactor trip modules. A trip in any two of the four protection channels initiates a trip of all four logic networks.

Each of the reactor trip modules controls a CRDCS trip device. Thus, a trip in any two of the four protection channels initiates a trip of all the CRDCS trip devices. The power trip devices, however, are arranged in a "one-out-of-two taken twice" logic system.

Before any reliability analysis can be performed, the system to be analyzed must be explicitly defined and what is meant by a failure must be clearly specified.

In this study the action of the safety shutdown system can be one of two functions: either the safety system shuts down the reactor when a situation arises that requires reactor shutdown, or the safety system does not shut down the reactor when nothing is wrong.

Because the reliabilities encountered are often very close to 1.0, it is more convenient to talk in terms of failure probabilities. In this context, failure probability is defined to be, "the probability that a system, subsystem or component will suffer a defined failure in a specified period of time."⁸

In this study the system to be analyzed includes all the sensing instruments and their associated equipment that monitor plant parameters, the protection system logic, the devices that provide shutdown signals to the control rods and all power supplies for the components listed above. The system does not include the control portion of the CRDCS which positions the reactor control rods or the latching mechanisms which hold the control rods in place ready for a free-fall gravity trip. Schematically, this is the system represented by Figures 7.2-1 and 7.7-4 of reference 4.

It is also necessary to specify the type of accident being analyzed because each sensor is only designed to protect against

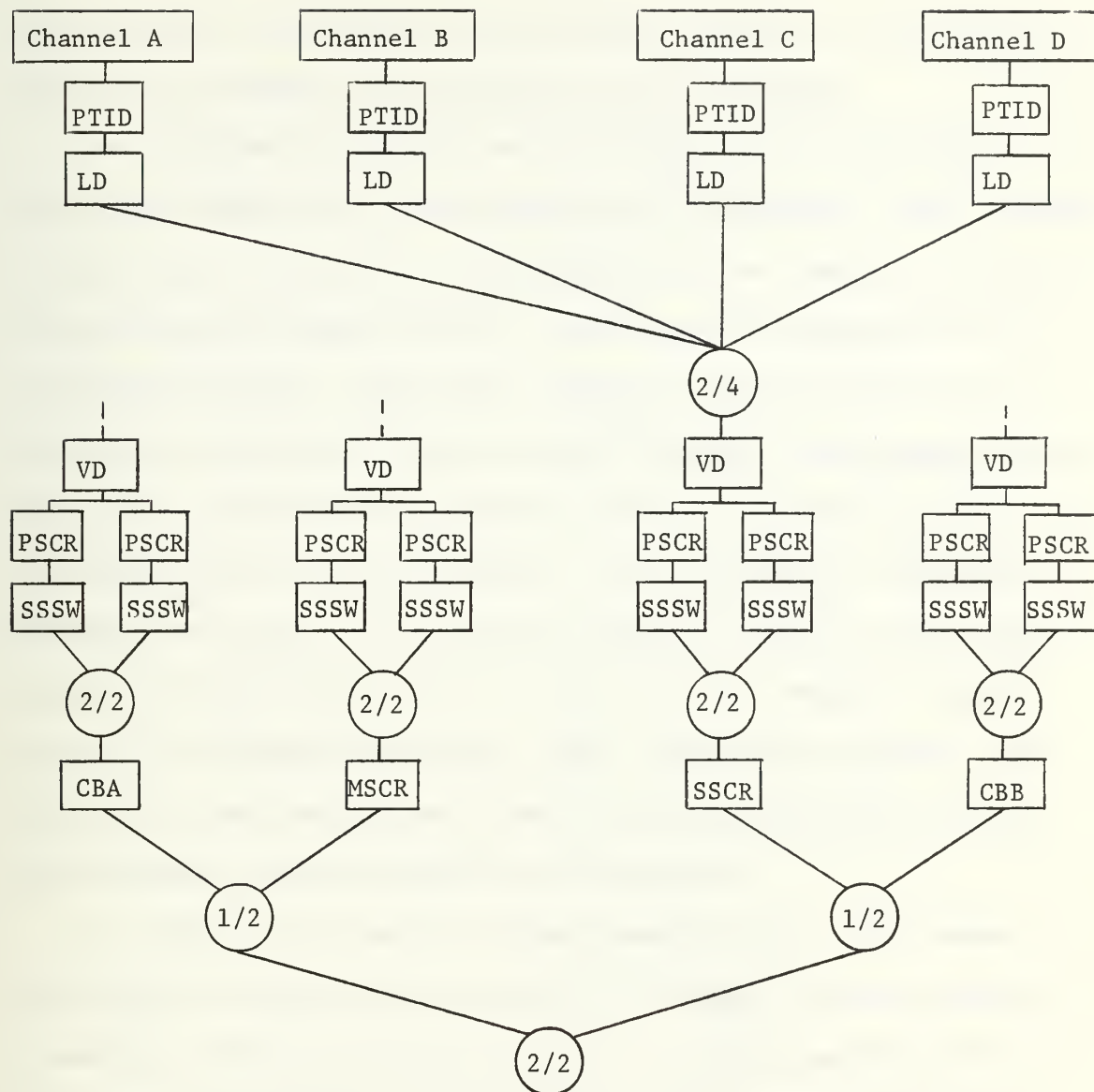
certain accidents. For example, the ion chambers will not protect against a loss of coolant accident.

The method of analysis used in this study is identical to the method employed in reference 9. Four basic steps are followed and are summarized below:

1. The system is qualitatively analyzed, component by component, for types of failures that can occur and what effect these failures have on the system.
2. A reliability block diagram is constructed.
3. Failure rate data or estimates are obtained.
4. Numerical calculations are performed to determine a failure probability for the repair interval specified.

As previously indicated, this study will look at the safety shutdown system from two failure probability viewpoints: fail-to-danger failure probability (safety shutdown system failure); and false scram failure probability of the shutdown system. Additionally, the fail-to-danger failure probability will be broken down into two specific accidents: loss of coolant and overpower.

With the types of failure probabilities now specified, steps 1 and 2 listed above can be executed. Each component of Figure 7.2-1 and the CRDCS trip portion of Figure 7.7-4, both of reference 4, was analyzed for its applicability to that type of failure and a reliability block diagram was formed. Figure 1 shows the resulting reliability block diagram for the fail-to-danger failure probability, while Figure 2 is the reliability diagram obtained for the false scram failure probability. It is pointed out that the logic combinations $1/m$ and $1/n$ on Figure 1 are general expressions, and the exact



Legend

See Table 1

Figure 1. (cont.)

configuration is determined by the accident specified. This will be discussed in greater detail further on in the analysis.

As previously described, the RPS consists of four identical protection channels which are redundant and independent. When combined in the system's logic, they automatically trip the reactor to protect the core and the coolant system. Each channel is served by its own independent sensors. Each sensor supplies an input signal to one or more signal processing strings in the RPS channel. Each signal processing string terminates in a bistable which electronically compares the processed signal with trip setpoints. All bistable trip outputs are connected in series. In the normal, untripped state the output associated with each bistable will be closed, thereby sending a constant signal to the Channel Trip Memory (CTM). Referring to Figure 1 and Table 1, a brief description of each trip initiating circuit for the fail-to-danger failure probability is presented:

1. High and low reactor coolant pressure trip - Each channel monitors the reactor coolant pressure. The signal from the pressure transmitter (RCPX) is processed and fed to a buffer amplifier (B1). The signal is then sent to both the high and low pressure bistables (HPBS, LPBS). If the pressure signal exceeds the high pressure trip setpoint or is lower than the low pressure trip setpoint, the appropriate bistable will trip causing the channel to trip.

2. High and low pressurizer level trip - Each RPS channel also monitors the pressurizer level. The signal from the differential pressure (level) transmitter (dPLX) is processed and fed to a buffer amplifier (B2). The signal is then sent to the high and low pressurizer level bistables (HZBS, LZBS). If the pressurizer level

Table 1

Legend for Reliability Block Diagrams

Symbol	Component
AMP	Amplifier
B1, B2	Buffers
BU1, BU2, BU3, BU4	Bridge Completion Units
CBA, CBB, CBE	Circuit Breakers
CM	Calculating Module
CPS	Calculating Module Power Supply
CTM	Channel Trip Memory
dPFX	dP Flow Transmitter
dPLX	dP Level Transmitter
DFA	Differential Amplifier
GD	Gate Drive
HABS, HBBS	High Temperature Bistables
HPBS	High RC Pressure Bistable
HZBS	High Pressurizer Level Bistable
HVPS	High Voltage Power Supply
ICH	Ion Chamber High
ICL	Ion Chamber Low
KLS	Key Lock Switch
LA	Linear Amplifier
LD	Line Driver
LPBS	Low RC Pressure Bistable
LZBS	Low Pressurizer Level Bistable
MI	Module Interlock
MRGD	Main Motor Return Gate Drive
MPS	Main 440V Power Supply
MSCR	Main 440V Power Supply SCR's
OPBS	Overpower Bistable
OPEC	Optical Encoder
ORG	OR Gate
PFBS	Power/Flow Bistable
PSCR	Photo SCR Isolation Device

Table 1 (cont.)

Symbol	Component
PTID	Photo Transistor Isolation Device
RCPX	RC Pressure Transmitter
RS	Reset Switch
RTD1, RTD2, RTD3, RTD4	RTD's
RLY	Relays
SA	Summing Amplifier
SBSW	Shutdown Bypass Switch
SC	Signal Converter
SCR	Silicon Controlled Rectifier
SQX	Square Root Extractor
SPS	Secondary 440V Power Supply
SSCR	Secondary 440V Power Supply SCR's
SSSW	Solid State Switch
TC	Test Circuit
TPS	Third 440V Power Supply
VBA, VBB, VBC, VBD, VBE	Vital Buses
VD	Voter Device
XMFR	Transformers
24PS	24V DC Power Supply (SCR's)

exceeds the high level trip setpoint or is lower than the low level trip setpoint, the appropriate bistable will trip causing the channel to trip.

3. High outlet temperature trip - Each channel monitors the temperature of both RC outlet loops. The signal from each resistance temperature detector (RTD3, RTD4) is sent to separate matched bridge networks (BU3, BU4) and fed to a signal converter (SC) which also acts as an isolation device. The loop A and loop B outlet temperature signals are then sent to separate high temperature bistables (HABS, HBBS). If the temperature signal exceeds the high temperature trip setpoint, the bistable will trip causing the channel to trip.

4. Overpower trip - Each channel also monitors the flux in a quadrant of the core. Signals from each half of a two section, out-of-core, uncompensated ion chamber (ICH, ICL) are sent to separate linear amplifiers (LA). The signals proportional to the neutron flux in the top and bottom halves of the core are then summed in a summing amplifier (SA) which also acts as an isolation device. The total power signal is then sent to the overpower bistable (OPBS). If the total power signal exceeds the overpower trip setpoint, the bistable trips causing the channel to trip.

5. Power/Flow trip - Each RPS channel monitors the total RC flow. A differential pressure transmitter (dPFX) measures the pressure drop across the core and provides a signal, proportional to the flow squared, to a square root extractor (SQX). The signal from the extractor is then sent to an amplifier (AMP) to produce a total flow signal. The amplifier also acts as a scaling amplifier and isolation device. The scaled total flow signal is then sent to the power/flow

bistable (PFBS). The total reactor power signal discussed in 4 is also sent to the power/flow bistable. If the total power signal exceeds the total reactor coolant flow signal scaled by the power-to-flow ratio trip, the power/flow bistable will trip causing the channel to trip.

6. Calculating module trip - The calculating module (CM) provides the offset, low DNBR and power/ ΔT (used only during startup) trip functions. The calculating module utilizes analog and digital signals processed by the RPS instrumentation channels as input. The input signals used by the module are:

a. The reactor coolant pressure signal from the buffer amplifier used by the high and low pressure trip bistables discussed in item 1.

b. The two reactor coolant inlet temperatures monitored by RTDs (RTD1, RTD2). The signals from each RTD are sent to a separate matched bridge network (BU1, BU2) and fed to a signal converter (SC) which acts as an isolation device.

c. The two reactor coolant outlet temperature signals from the signal converter used by the high temperature trip bistables discussed in item 3 above.

d. The neutron flux signal in the bottom half of the core is subtracted from the flux signal for the top half of the core in a difference amplifier (DFA). The imbalance signal is then inputted to the calculating module.

e. The total power signal from the summing amplifier (SA) discussed in item 4.

The calculating module then provides the following trip signals to the calculating module bistable (CMBS):

a. Offset trip - This trip prevents the core from operating with axial power distributions that could cause the local linear heat rate to exceed the kW/ft safety limit. The offset trip lines are intended to provide offset protection for only the power levels that can be reached without activating the overpower trip or the power/flow trip bistables.

b. Low DNBR trip - The low DNBR trip prevents the reactor from operating in a steady-state condition below the minimum allowable DNBR.

c. Power/ ΔT (Startup) trip - If the total reactor power signal exceeds a preset value and the differential temperature across the reactor core (ΔT) is less than a preset value, the calculating module provides a trip signal to the bistable.

Any one of these trip signals will trip the bistable which in turn will trip the channel.

In the event there is a trip of one of the discussed bistables, the signal to the Channel Trip Memory (CTM) in that channel will be interrupted. The channel trip memory can only be reset through use of a reset switch (RS) by deliberate operator action once the trip condition has cleared. The channel trip memory will then send a constant trip signal to a line driver (LD) which is isolated from the trip memory by a photo-transistor isolation device (PTID). At this point on the reliability diagram, the four channels are brought together in four two-out-of-four logic voter devices. Since voter devices are

not perfect devices, the voter can be regarded as two series elements consisting of a perfect logic circuit in series with the actual components used in the formation of the logic²². Each logic network is separated from a solid state switch (SSSW) by a photo SCR isolation device (PSCR). The switch provides 120 volt AC power to the under-voltage coils on the main and secondary 440 volt power circuit breakers (CBA, CBB) and to the electronic type relay coils in the main and secondary SCR circuits. For a reactor shutdown, both solid state switches in each channel are required to be switched off, thereby cutting power to the circuit breaker coils or the SCR circuit electronic type relay coils.

As previously indicated, the power trip devices are arranged in a "one-out-of-two taken twice" logic system. This arrangement has circuit breaker A and the main SCR circuit linked in series, while circuit breaker B and the secondary SCR circuit are in series. Thus for a reactor shutdown, one power trip device from each series must be tripped.

Figure 2 depicts the false scram reliability diagram. In this diagram, all sensors and their signal processing strings are connected in series since a failure of one component can cause the channel to trip. The remaining portions of the system after the Channel Trip Memory (CTM) are identical to that previously discussed, except for the logic combinations and the inclusion of the vital buses (VBA, VBB, VBC, VBD), the 440 volt power supplies (MPS, SPS) and the step down transformers (XMFR). The logic required at the channel level is three-out-of-four since at least three channels in a non-tripped state are

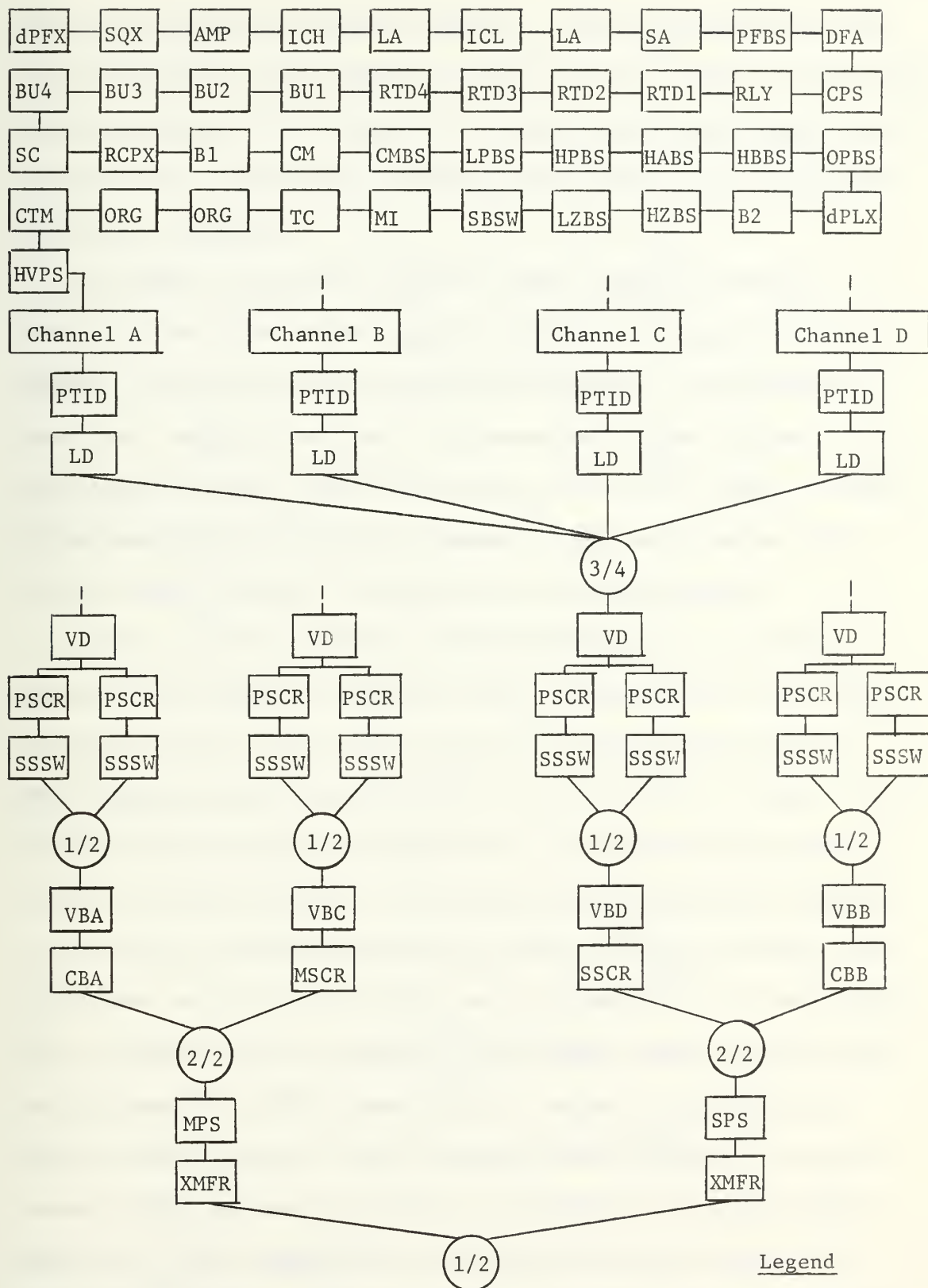
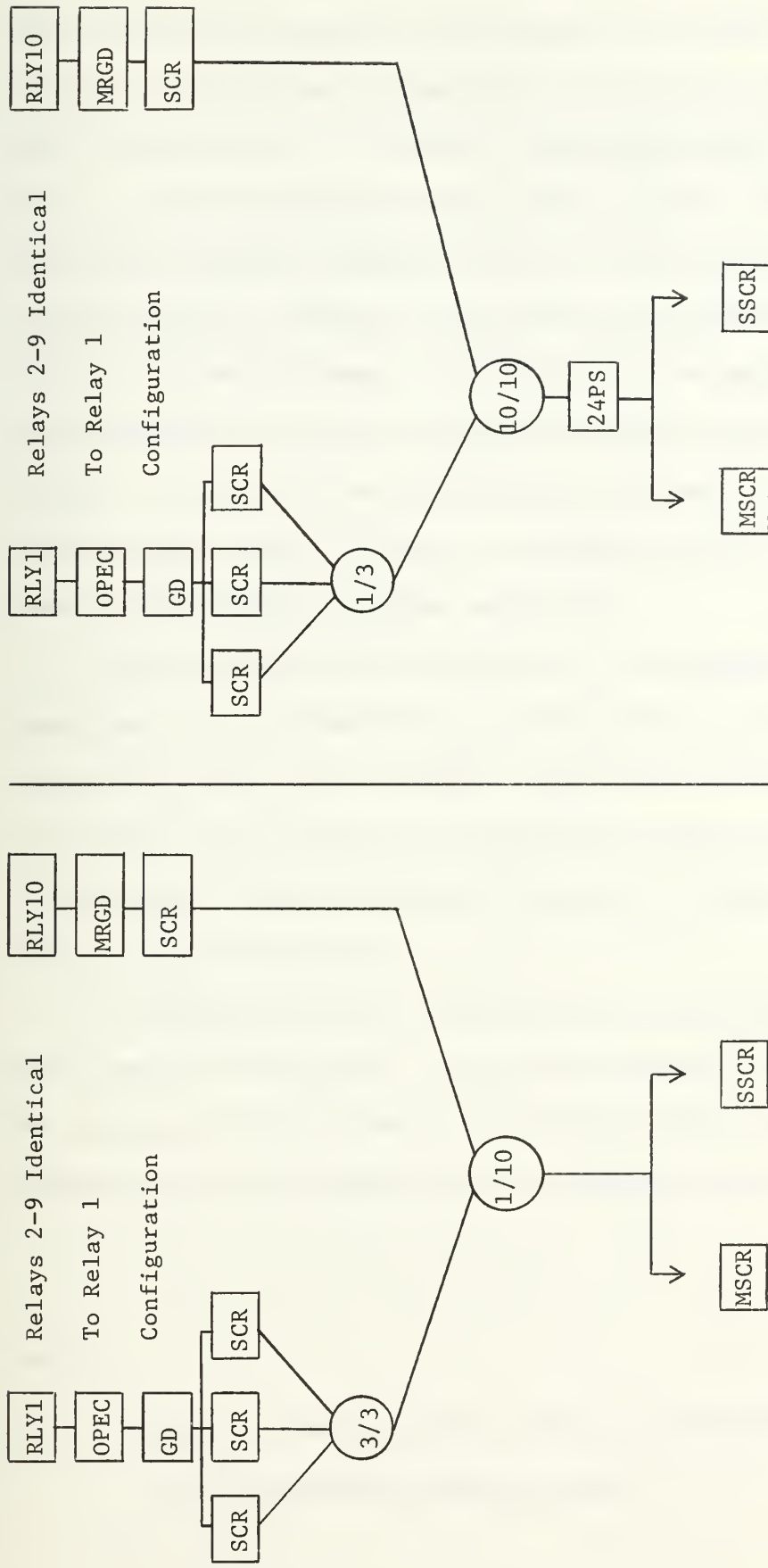


Figure 2. False Scram Reliability Diagram for Babcock-241 NSS Automatic Safety Shutdown System

required for continued reactor operation. The logic required at the solid state switch level (SSSW) is one-out-of-two, since one non-tripped switch supplying 120 volt AC power to either the circuit breaker under-voltage coils or SCR circuit electronic type relay coils is required for reactor operation.

The power trip devices (CBA, CBB, MSCR, SSCR) are arranged in a "one-out-of-two taken twice" logic in the fail-to-danger reliability diagram. In the false scram reliability diagram, a "two-out-of-two taken once" logic is required. This means that either the power train with circuit breaker A (CBA) and the main SCR circuit (MSCR) in series or the power train with circuit breaker B (CBB) and secondary SCR circuit (SSCR) in series is required for reactor operation.

Figure 3 gives a detailed reliability diagram for the blocks labeled MSCR and SSCR on Figures 1 and 2. Figure 3a is for the fail-to-danger failure, while Figure 3b is for the false scram failure. These figures depict the second method of interruption of power to the control rod drive mechanisms (CRDM), the first being the previously discussed circuit breakers. In this method the gate control signals to the silicon controlled rectifiers (SCRs) in each of the nine CRDM group power supplies and the motor return power supply are interrupted. The trip devices are ten electronic type relays connected with their coils in parallel (RLY1 through RLY10). Contacts of these relays serve to remove the gate control signals passing through the optical encoder (OPEC) and gate drive (GD) to the SCRs in each power supply. Because the power supplies have redundant halves, two sets of ten relays are provided. The trip relays can remain in their non-tripped



a. Fail-to-Danger

b. False Scram

Figure 3. Reliability Diagram Main and Secondary Power SCR's

state only if the associated trip channel is energized. For the configuration depicted in Figure 3a, interruption of only one relay out of the ten shown is required. Conversely, Figure 3b indicates that all ten relay configurations must work to prevent a false trip signal from being propagated further on in the shutdown system. It should be noted that for purposes of this study, the ganged manual trip switches (S1 and S2) shown on Figure 7.2-1 of reference 4 have been neglected since the area of interest is in the automatic shutdown circuit. In a more extensive reliability analysis of the system, these switches would be taken into account along with the failure rate associated with the human operator^{5,8}.

With the reliability block diagrams now formulated for the specified failure probabilities, failure rates for each component on these diagrams can be assigned. Based upon the data accumulated in Appendix I and justified in Appendix II, Table 2 assigns the failure rates to the components of Figures 1-3 (identified in Table 1) for the specific failure.

Two components remain to have failure rates assigned, the OR gates and the voter device. For these components a failure rate can be calculated from the formulas of MIL-HDBK-217B, reference 10. The failure rate is calculated from the expression given on page 2.1.1-1

$$\lambda_P = \pi_L \pi_Q (C_1 \pi_T + C_2 \pi_E) \quad (1)$$

where

λ_P is the device failure rate in failures/ 10^6 hrs.

π_L is the device learning factor

Table 2

Failure Rates Used in Analysis

Component	Failure Rate (failures/ 10^6 hrs.)	
	Fail-to-Danger	False Scram
AMP, B1, B2, DFA, GD, LA, LD, MRGD, SA, SQX	5	5
BU1, BU2, BU3, BU4	1	1
CBA, CBB	10^{-3} /demand	1
CM	5	0.5
CTM, HPBS, HZBS, HABS, HBBS, LPBS, LZBS, OPBS, OPEC, PFBS, PSCR, PTID	1	0.1
dPFX	35	35
dPLX	15	15
HVPS, 24PS, CPS	--	10
ICH, ICL	50	50
KLS, RS	10^{-5} /demand	0.1
MI, SBSW	--	0.1
MPS, SPS, VBA, VBB, VBC, VBD	--	0.5
RCPX	25	25
RTD1, RTD2, RTD3, RTD4	15	15
RLY	0.01	0.1
SC	20	20
SCR	1	3
SSSW	3	1
TC	--	0.6
XMFR	--	1

π_Q is the quality factor

π_T is the temperature acceleration factor

π_E is the application environment multiplier.

C_1 , C_2 are the circuit complexity factors. All of the factors are available in tabular form in reference 10 and the following values are assigned:

$$\pi_L = 1.0 \text{ (Table 2.1.5-2)}$$

$$\pi_Q = 10 \text{ (Table 2.1.5-1)}$$

$$\pi_T = 0.545 \text{ (Table 2.1.5-4 at } 60^\circ\text{C } T_j)$$

$$\pi_E = 1.0 \text{ (Table 2.1.5-3)}$$

For the OR gate, the values for C_1 and C_2 are 0.0013 and 0.0039 respectively. For the voter device (in the proposed Babcock-241 NSS design this is a two-out-of-four logic device containing seven gates), C_1 and C_2 are assigned the values 0.0048 and 0.0078 respectively. These values are obtained from Table 2.1.5-5 of reference 10. Using these values and equation (1), failure rates for the OR gate (ORG) and voter device (VD) are calculated to be 5×10^{-8} failures/hr. and 1.0416×10^{-7} failures/hr. respectively.

With failure rates assigned to each component in Figures 1-3, step four of the method of analysis, the numerical calculation of a failure probability for the automatic safety shutdown system, can be performed. Prior to this though, a number of additional assumptions must be stated. These additional assumptions and others previously discussed are:

1. Failures are statistically independent and no common mode situations exist. In general this is not true, but for purposes of this study, this is assumed.

2. Any voter or voter-switch can be regarded as a series element in the reliability block diagrams.

3. Channels are identical.

4. Channels are either good or bad. There is no intermediate state.

5. The hazard rates (instantaneous failure rates) associated with the components and channels are constant which gives rise to the exponential distribution for all subsequent reliability calculations.

Using conventional reliability analysis procedures for independent processes¹⁰⁻¹⁵, the component blocks on the reliability diagrams can be combined until a failure probability for the system defined is found as a function of some specified time interval. The reference to a specified period of time is extremely important. Reactor protection systems are periodically tested, inspected and repaired. If one can assume that all failures are instantaneously corrected at the end of the test interval, then that interval is also the repair interval over which the reliability calculations are made. Thus, for this study the test and repair interval is assumed to be the same and is referred to as the "repair interval."⁹ For plug-in type electronic circuit boards this is a reasonable assumption.

As indicated earlier, the fail-to-danger failure probability is being analyzed for two types of accidents: loss of coolant and overpower. Each accident will have a different logic combination in

the 1/m and 1/n logic circles shown on Figure 1. This is because each sensor is only designed to protect against certain accidents.

In the loss of coolant accident the 1/m logic becomes 1/1 since only the input from the reactor containment (RC) pressure detector train is utilized by the calculating module. The 1/n logic becomes 1/3 since only the inputs from the low pressurizer level bistable, low RC pressure bistable, and the calculating module bistable trains are involved. All other bistable trains are not associated with this accident.

Similarly, the logic for the overpower accident assumes the following form: the 1/m logic becomes 1/4 with both ion chamber trains and the two RTD trains associated with the coolant outlet temperature involved. The 1/n logic becomes 1/5 with the power/flow bistable, overpower bistable, both coolant outlet temperature RTD bistables, and the calculating module bistable trains participating. Again, all other components not associated with this accident are neglected. With these substitutions, a fail-to-danger failure probability for the automatic system for the two accidents as a function of repair interval time can be determined.

The results of the calculations for the fail-to-danger and false scram failure probabilities are presented in Figure 4. The false scram curve indicates a marked increase in the failure probability for a repair interval between 100 and 1000 hours. This is due to the fact that at low time intervals (<100 hours), the components in a channel with high failure rates such as the ion chambers ($\lambda = 50 \times 10^{-6}$ failures/hr), dominate the reliability calculations while the

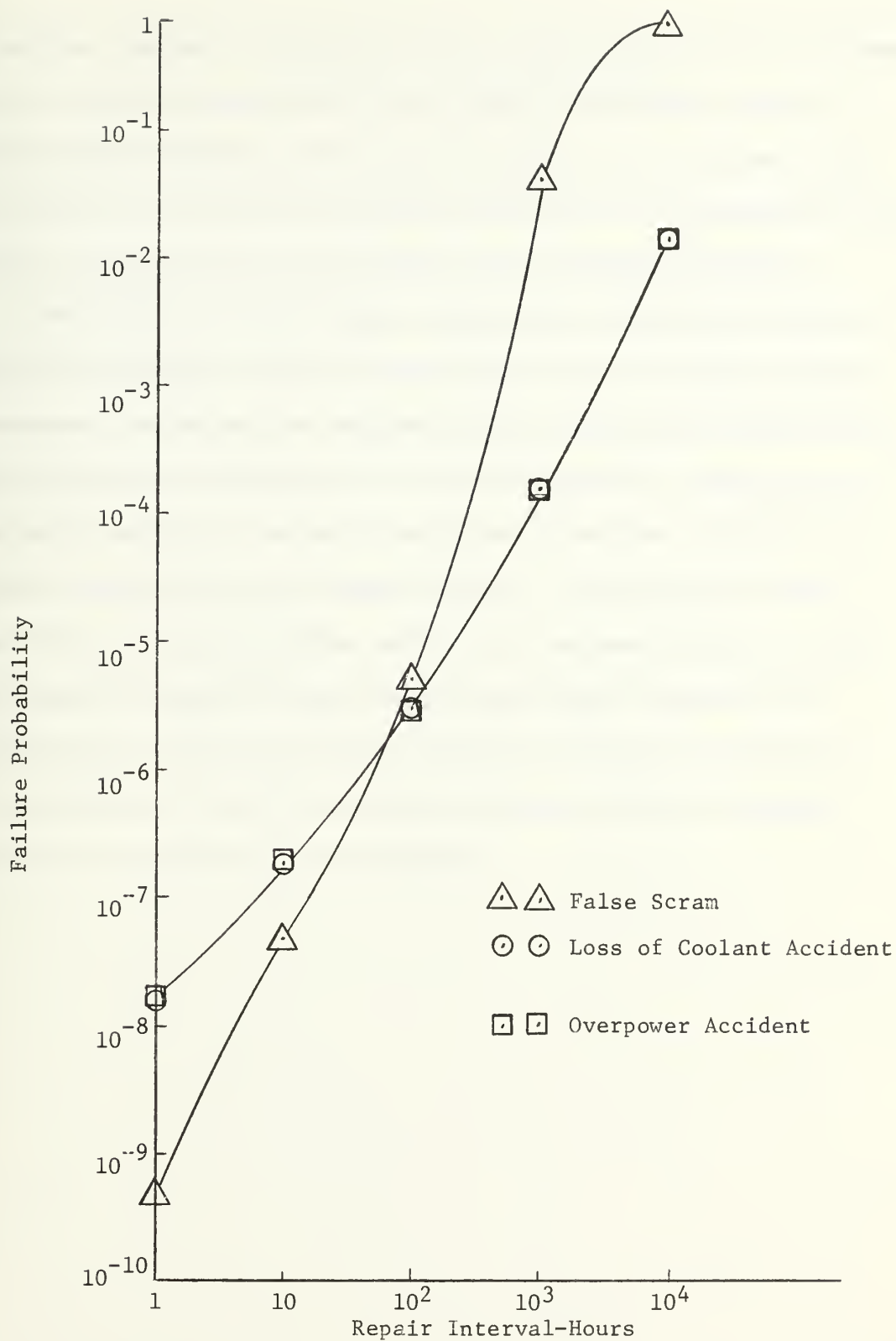


Figure 4. Babcock-241 NSS Automatic Safety Shutdown System Failure Probability vs. Repair Time Interval

remaining components contribute little. As the time interval increases, however, these components with low failure rates begin to play an increasingly important role in the reliability of the system. Thus, to decrease the false scram failure probability to an acceptable value at high time intervals would require ultra-reliable components.

Conversely, the two accident curves show no abrupt increase in their fail-to-danger failure probabilities over the repair intervals considered. As before the components with high failure rates dominate the reliability calculations at low time intervals. However, due to the logic combination unique to each type of accident specified, the failure probabilities are almost identical. So, in spite of the fact that the bistable trains used in the overpower accident contain a considerable number of high failure rate items, because of the combinational logic used for the accident, the failure probability is comparable to that of an accident employing different bistable trains with low failure rate components.

III. BACKGROUND OF LOW LEVEL LOGIC REDUNDANCY IN COMPUTER SYSTEMS

In this section, computer system fault masking logic redundant circuits are investigated for potential use in nuclear safety circuits. Not all circuits or devices investigated in the computer field are evaluated in this study; only those with the highest system reliability potential.

Bazovsky¹⁵ has shown that the highest reliability is obtained in redundant systems when the redundancy is at the lowest possible level. In computer systems this implies that the redundancy should be at least at the logic element level. Numerous investigators over the past 15 years have developed and analyzed several forms of computer and logic redundancy¹⁶⁻²¹, and the reliabilities of the various configurations have been summarized by Dennis²².

Table 3 made from the Dennis summary and using his notation indicates the various types of redundancy that have been studied in the space and computer industries. The configurations A to H are of increasing order of reliability and complexity. Most of the higher letter configurations have not been employed in nuclear safety shutdown circuits, but variations of Type C redundancy are commonly found.

For later comparison purposes, a more detailed description of the Type H voter-switch, the potentially highest reliability configuration, is now presented. This system is credited to Goldberg²³ and is sometimes referred to in the literature as a THISS (TMR/Hybrid/Single/Single) voter-switch²⁴. TMR refers to triple modular redundant and the basic TMR circuit is indicated in Table 3 as Type B. The

Table 3

Unreliability of Voters and Voter-Switches with Powered Standby Channels

Configuration	Description	Approximate Unreliability For Short Missions ($\lambda t < 0.5$) f = unreliability of a channel f_v = unreliability of a voter
Voter A Non-Redundant (k out of m)	A number of channels and a single voter whose output represents a strict majority vote. Common configurations use an odd number of channels such as 2 out of 3, or a 3 out of 5 vote.	$\frac{m!}{(m-k)!k!} f^k$
Voter B Redundant (k out of m)	Same as Type A except there are now m voters as well as channels. Common configuration uses $m = 3$ and is called TMR (Triple Modular Redundant) in computer industry.	$\frac{m!}{(m-k)!k!} (f_v^k + f^k)$
Voter-Switch C Adaptive Voter m channels	This is an adaptive or reconfigurable voter circuit. It eliminates channels as they fail and maintains its voting function during the elimination. It becomes inoperable when there is a disagreement between the two channels that finally remain. It can be configured with single or multiple voters. Common nuclear example is a 2 out of 4 system that degrades to a 1 out of 3.	f_m^{m-1}

Table 3 (cont.)

Configuration	Description	Approximate Unreliability For Short Missions ($\lambda t < 0.5$) f = unreliability of a channel f_v = unreliability of a voter
Voter-Switch D TMR Single	This TMR configuration starts off with 3 good channels. If one channel goes bad a logic device automatically disconnects it. At the same time the device automatically removes one of the remaining good channels leaving only a single channel path.	$\frac{3}{2}f^2$
Voter-Switch E TMR/Single/Single	This system is an extension of configuration D. After the sequence described in D above is complete, the discarded good channel is switched back into the circuit.	f^3
Voter-Switch F TMR/Hybrid with s spares	The TMR configuration is supplemented by spare standby channels. These spares are automatically switched in to replace failed channels. When the spare channels are used up, the system remains a basic TMR.	$(s + 3)f^{s+2}$
Voter-Switch G TMR/Hybrid/Single with s spares	The initial configurations are as indicated for Type F. After the spares are used up and the final TMR arrangement attained, the next channel failure switches out the bad channel and one good one leaving a single final good channel.	$\frac{s+3}{2}f^{s+2}$

Table 3 (cont.)

Configuration	Description	Approximate Unreliability For Short Missions ($\lambda t < 0.5$) f = unreliability of a channel f_v = unreliability of a voter
Voter-Switch H TMR/Hybrid/Single/ Single with s spares	This configuration is identical to Type G except the good channel previously discarded is finally used.	f^{s+3}
Note: Only the type B voter includes the reliability of the voter (p_v). All other circuits require that the effect of the voter reliability be included separately.		

incremental reliability gain as a function of the number of spares in the THISS configuration has been shown^{16,17} to rapidly decrease beyond two spare channels, and it is the operation of a THISS-2, a two spare combination, that will be examined. Figure 5 shows a possible life cycle of the system. Here originally channels A, B, and C are working and channels D and E are unconnected standby spares, and at this time may be either powered or unpowered. Figure 5 first assumes that channel C has failed. Actually any one of the original working channels may fail and the system will degenerate into a THISS-1. The next failure causes deterioration into the simple TMR arrangement (THISS-0) which is still triple voting. In other words, even after two failures the system still votes two-out-of-three. The THISS system will survive two more failures, but will no longer have the desired voting capability. Single channel operation only is provided after the spares are used up. The reason for switching from an effective three channel operation to a one channel system, rather than a two channel system, is because the single channel has a higher reliability. If two channels are used in a two-out-of-two configuration there simply would be twice as many components involved as in the single channel and given the same component failure rates, the reliability must be reduced. A one-out-of-two configuration is unsuitable in that there is the problem of knowing which channel is correct in the event of a failure. As is, the single channel can no longer rely on simple comparison diagnostics to determine proper switching operation, but must use additional techniques such as redundant coding.

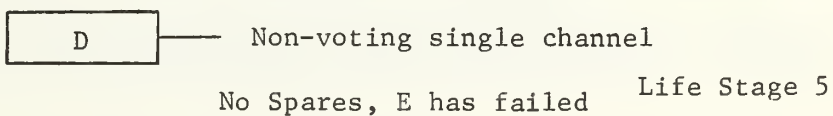
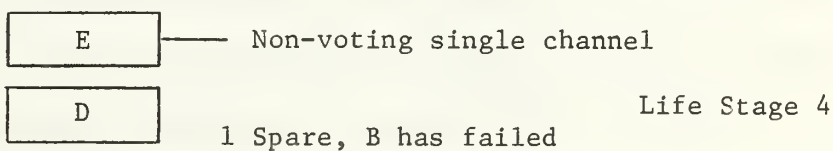
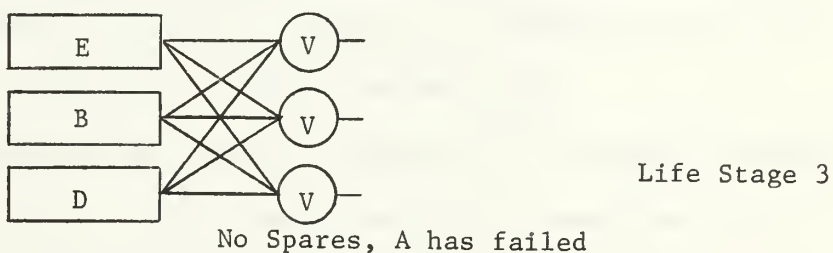
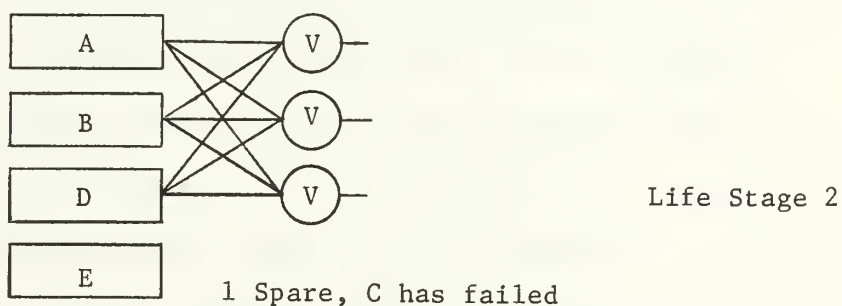
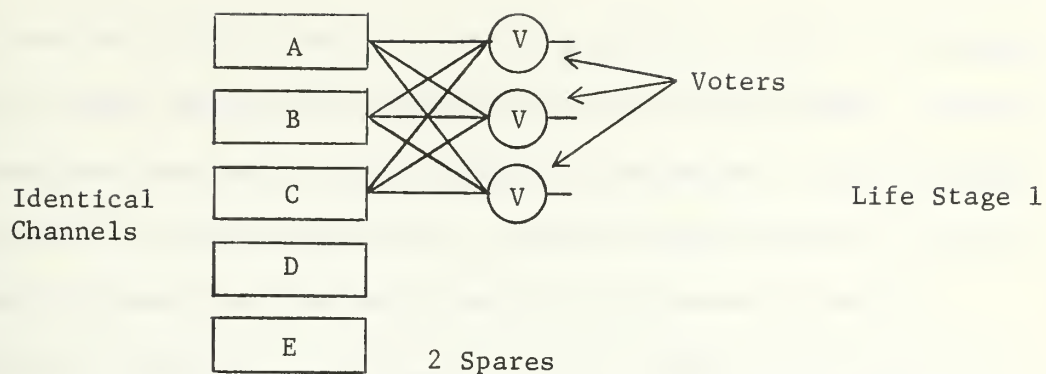


Figure 5. Life Stages of a THISS-2 Voter-Switch

With any form of hard-wired working majority voters all channels obviously must be powered. However, when switchable standby channels are employed they may be either powered or unpowered. The principal difference is in the failure rate. Powered channel failure rates are generally higher than unpowered ones with references 25 and 26, indicating that $\lambda_{\text{unpowered}}$, (λ_{up}) is of the order of 10 to 30% of λ_{powered} , (λ_{p}). The approximate unreliabilities indicated in Table 3 are for channels including spares fully powered. For the THISS-2 circuit having a perfect switching circuit this condition leads to the unreliability of f^5 where f is the unreliability of a single channel. Dennis further shows that if λ_{up} for a channel is 0 in the unpowered standby situation, then the THISS-2 system unreliability would only be reduced to $9/40 f^5$. And for λ_{up} between 0 and λ_{p} one might use linear interpolation without serious error.

The reliability of the switch is crucial in all standby redundancy situations. In computer terms this reliability is sometimes called coverage. There coverage is defined as the probability, given that a fault has occurred, that the fault will be detected in time to prevent the loss of significant information or function^{22,24}. For the relatively slow nuclear service, coverage may be considered simply as switch reliability, and uncoverage as switch unreliability or failure probability.

Reference 24 indicates the extreme sensitivity of the THISS-2 logic system to uncoverage. An approximate formula is developed (for $\lambda t < 0.4$) that indicates that the system unreliability

$$F \approx 3f_c f + 9/40 f^5 \quad (2)$$

where

F = the system unreliability

f = the original channel unreliability, and

f_c = the uncoverage, or switch unreliability.

It can be seen that the switch must be highly reliable in order for the overall redundant system to achieve its promised reliability. The second term of equation (2) as previously indicated represents the unpowered, perfect switch, system reliability. In order for the first term not to dominate, f_c must be on the order of f^4 , calling for the switch to have extreme reliability especially if the original channel reliability is high. Fortunately the switch can be a relatively simple solid state integrated circuit. Two generic types of switching may be employed. The first may be considered to be a brute force solution using only discrete logic elements, whereas the second solution employs the technique of logic through memory²⁷⁻³⁰. Integrated circuits of this sort may be carefully built and inspected to have failure rates between $\lambda = 10^{-8}$ to $10^{-9}/\text{hr}$ ^{10,31}. Hence considerable improvement in system reliability may be obtained over single complex channels employing process detectors, analog networks, A to D converters, and finally a micro-processor all effectively connected in series if these types of voter-switches can be used as low level logic elements.

IV. RECONFIGURATION OF BABCOCK-241 NSS SAFETY SHUTDOWN SYSTEM

In order to evaluate the failure probability of a safety shutdown system containing one of the higher lettered voters/voter-switches listed in Table 3, Figures 1 and 2 must be modified to include a fifth channel and power interruption device.

The fifth channel to be added will be designated channel E and is identical to the first four channels (A, B, C, and D) shown on Figures 1 and 2. In addition, a third source of 440V power, designated TPS, must be added and is connected to both the main and secondary 440V power supply circuits shown on Figure 7.7-4 of reference 4. The power trip device associated with this third 440V power supply is assumed to be a circuit breaker which is labeled CBE.

At this point, the voter or voter-switch to be included in the modified reliability block diagrams must be chosen. For comparison purposes with the two-out-of-four system, a three-out-of-five voter and the THISS-2 voter-switch previously discussed are chosen. Figures 6 through 9 are the resultant reliability diagrams for the fail-to-danger and false scram failure probabilities.

Figures 6 and 7 are, respectively, the reliability diagrams for the three-out-of-five voter fail-to-danger and false scram failure modes. Figures 8 and 9 are, respectively, the fail-to-danger and false scram reliability diagrams for the THISS-2 voter-switch.

Figure 8 requires some additional discussion. As indicated on the reliability diagram, the THISS-2 voter-switch is a four-out-of-five voter. The reason for this is because the THISS-2 voter-switch can

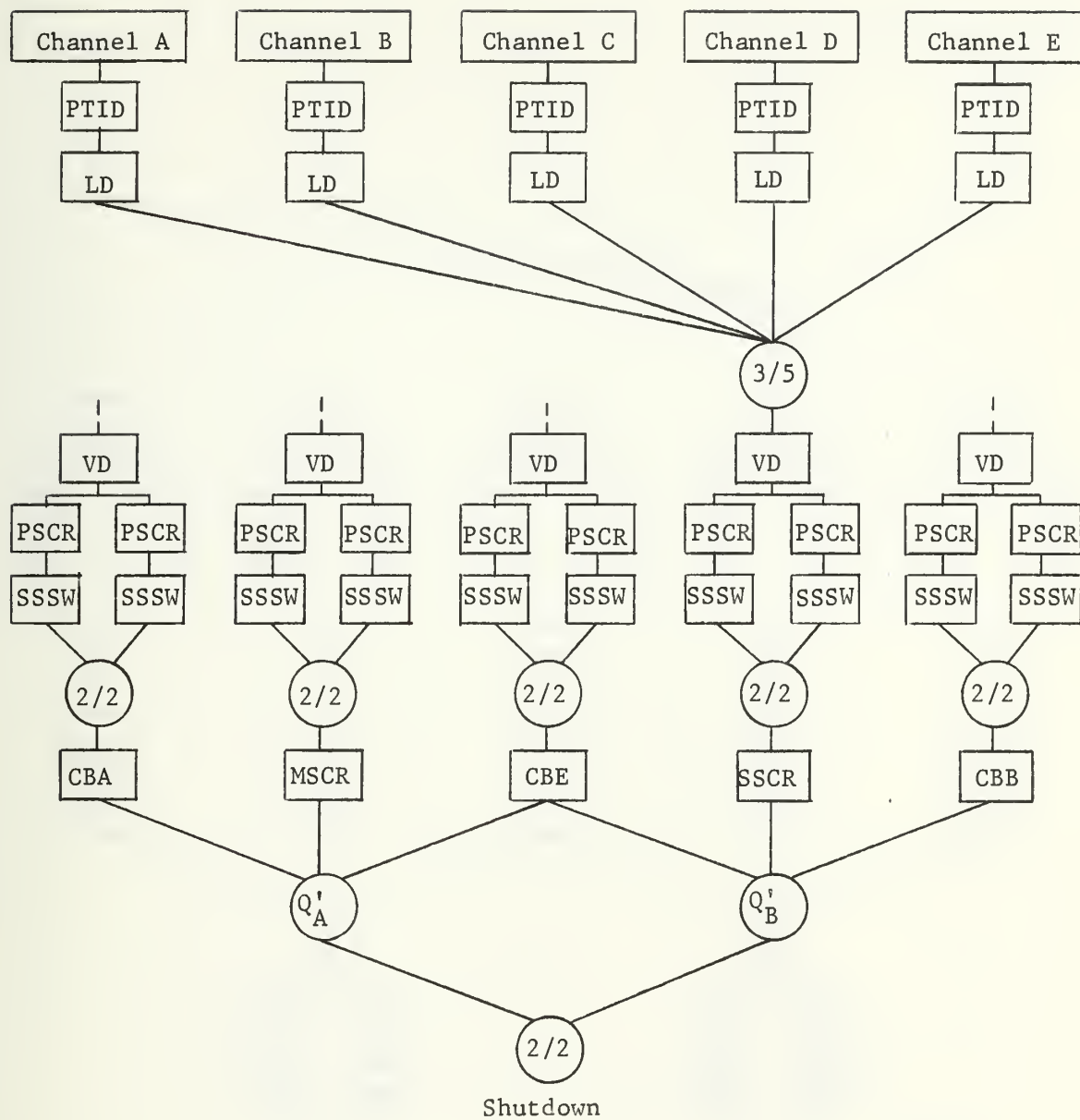
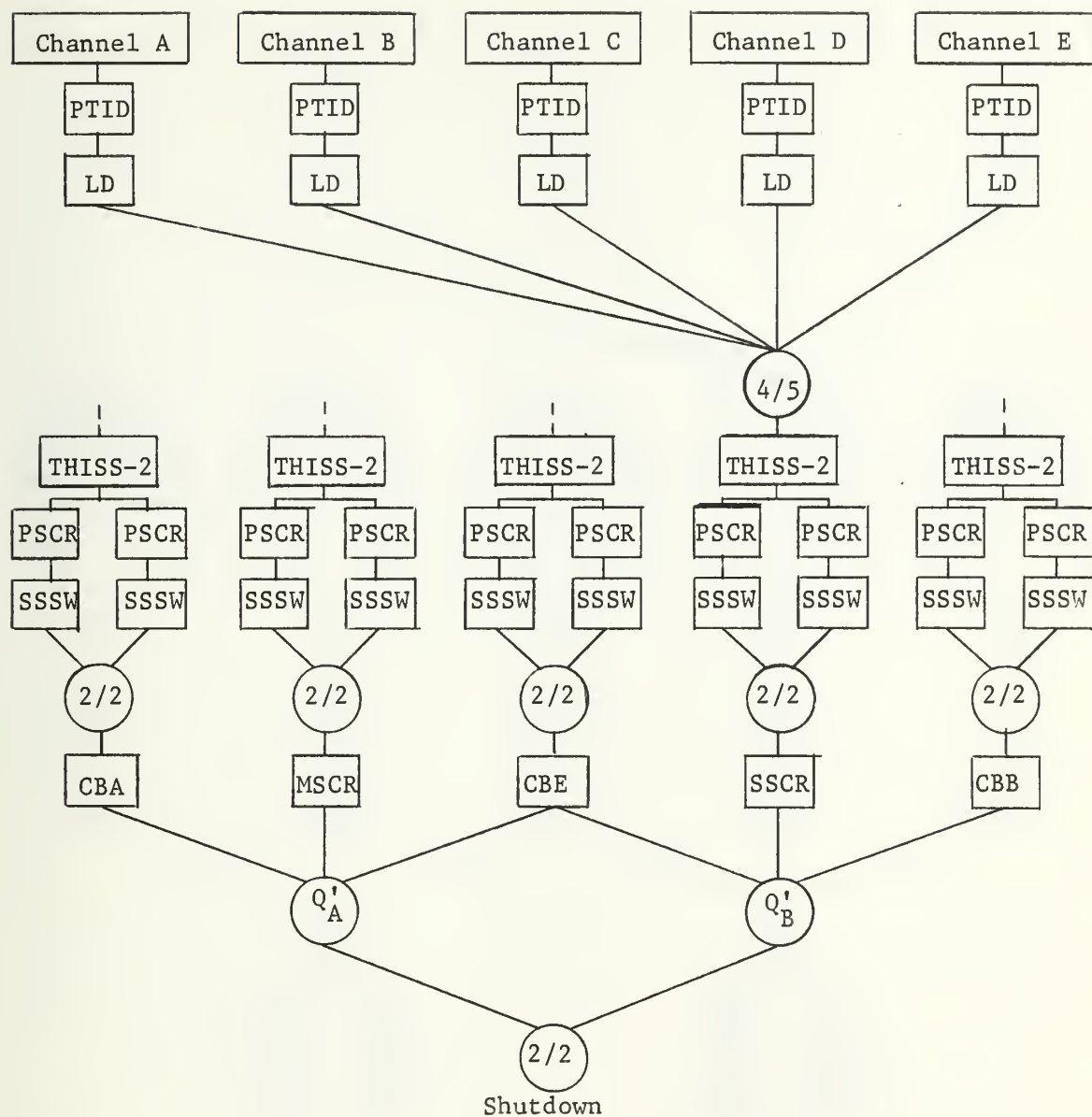


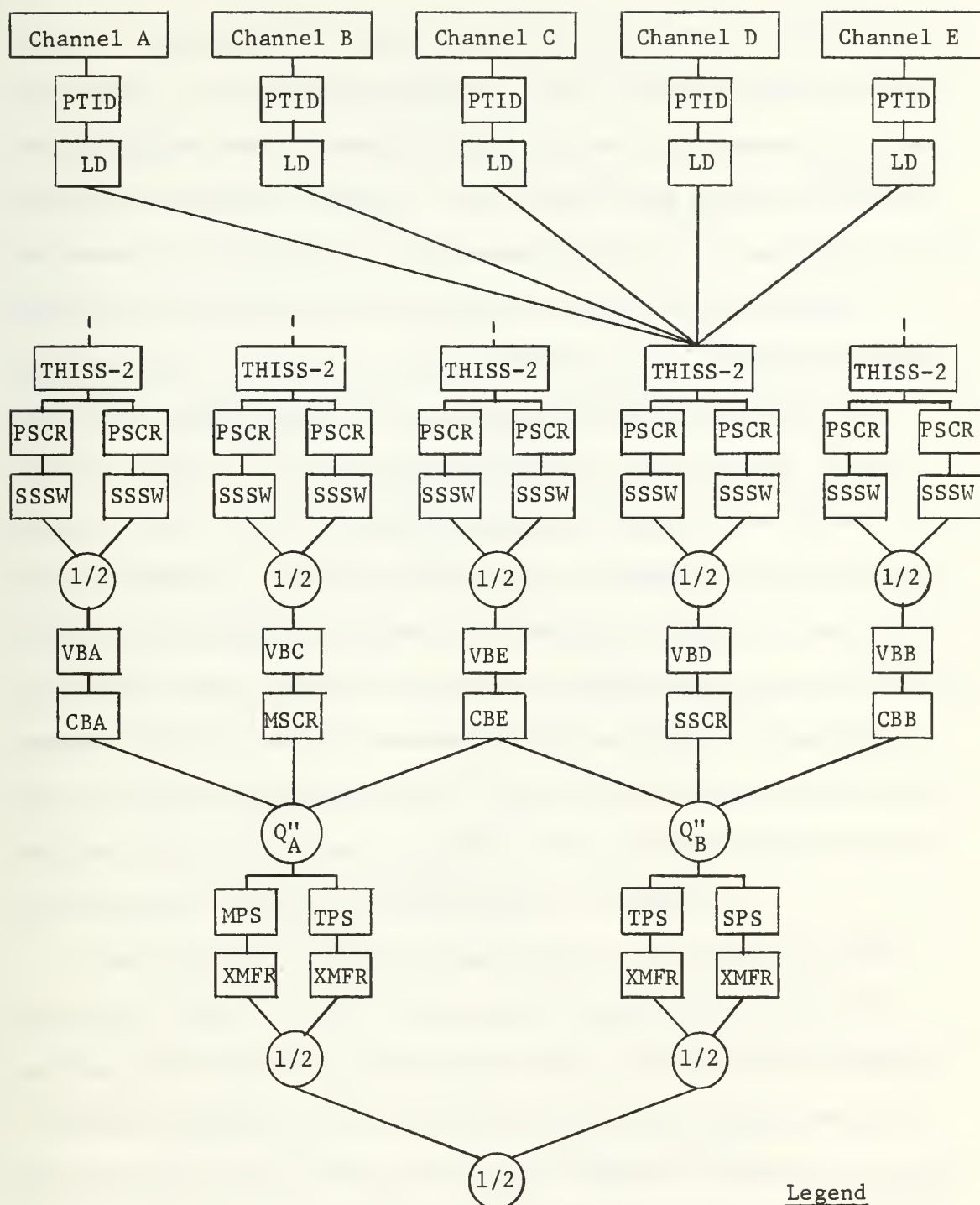
Figure 6. Fail-to-Danger Reliability Diagram for Automatic Safety Shutdown System with Three-out-of-Five Voter Device



Legend

See Table 1

Figure 8. Fail-to-Danger Reliability Diagram for Automatic Safety Shutdown System with THISS-2 Voter-Switch



Legend
See Table 1

Figure 9. False Scram Reliability Diagram for Automatic Safety Shutdown System with THISS-2 Voter-Switch

tolerate only at most one undetected failure and still operate in a safe manner. Two undetected failures will cause the voter-switch to switch out the wrong channel, in this instance the channel which has detected a dangerous condition. This comes about because switching is caused by the output of a difference detector. If any input to the switch is different than the output, then the differing channel is switched out. At this point the voter-switch has unwittingly incapacitated itself when needed if two previously undetected faults have existed. Even if the voter-switch switches in the standby channels one at a time, the two undetected failures cannot be overridden by the new channels. In fact, the switched in channels will be rejected as they are switched in, eventually leaving the safety system with a non-voting single channel containing an undetected failure as the only channel. This is best represented by Figure 10 which illustrates this key point against the THISS-2 voter-switch. For the false scram failure this problem does not exist. The voter-switch works exactly as discussed in section III and depicted in Figure 5.

Even though the logic has been changed at the channel voting level, the "one-out-of-two taken twice" feature of the CRDCS trip portion of the ESFAS of the original safety system has been retained. A modified expression for the logic at the point where blocks CBA, MSCR and CBE and CBB, SSCR and CBE come together is required, however. A truth table is constructed with a reliability expression written from the results. For the fail-to-danger failure mode the truth table (see Appendix III for truth tables) provides the failure probability expressions

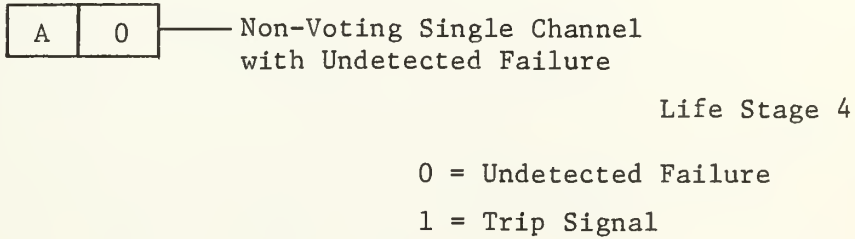
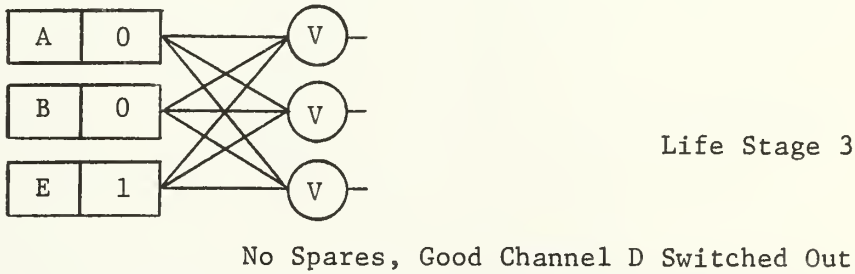
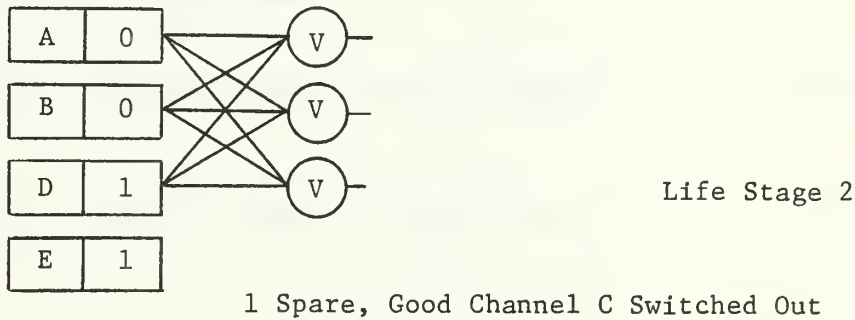
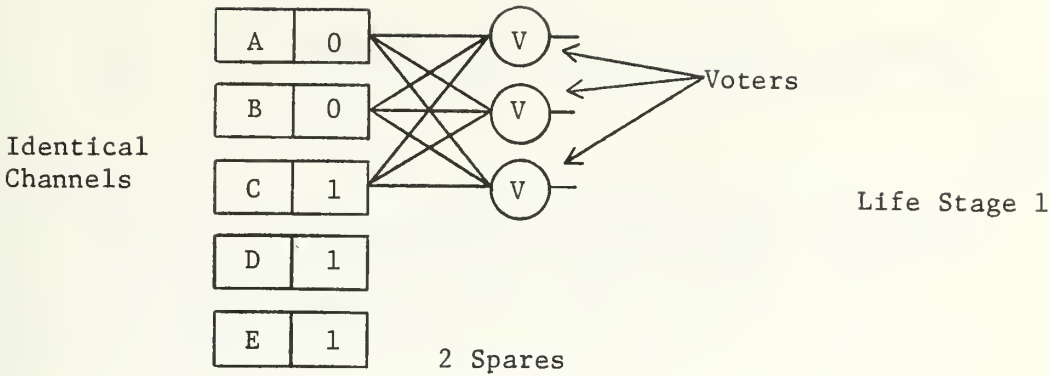


Figure 10. Life Stages of a THISS-2 Voter-Switch with Two Undetected Failures

$$Q'_A = 1.0 - \{(1-Q_A)^2(1-Q_C) + 2Q_A(1-Q_A)(1-Q_C) + Q_C(1-Q_A) + Q_A^2(1-Q_C)\} \quad (3)$$

$$Q'_B = 1.0 - \{(1-Q_B)^2(1-Q_D) + 2Q_B(1-Q_B)(1-Q_D) + Q_D(1-Q_B) + Q_B^2(1-Q_D)\} \quad (4)$$

Similarly, the truth table for the false scram failure gives rise to the failure probability expressions

$$Q''_A = 1.0 - \{2Q_A(1-Q_C)(1-Q_A) + (1-Q_A)^2(1-Q_C)\} \quad (5)$$

$$Q''_B = 1.0 - \{2Q_B(1-Q_D)(1-Q_B) + (1-Q_B)^2(1-Q_D)\} \quad (6)$$

V. NUMERICAL ANALYSIS OF MODIFIED SAFETY SHUTDOWN SYSTEMS

The numerical analysis procedure necessary to determine a failure probability value for the reliability diagrams shown as Figures 6, 7, 8 and 9 is identical to that in section II. Failure rates are assigned to each component block on the reliability diagrams using the values listed in Table 2. Equations (3), (4), (5) and (6) are used for the modified CRDCS trip trains. For the voter/voter-switch in each reliability diagram, a failure rate is calculated using equation (1) of section II with the exception that the three-out-of-five voter contains 11 gates and the THISS-2 voter-switch is assumed to be equivalent to 100 gates. From Table 2.1.5-5 of reference 10, C_1 and C_2 for the three-out-of-five voter are assigned the values 0.0065 and 0.0092 respectively. Table 2.1.5-7 of reference 10 assigns the values of 0.030 and 0.020 to C_1 and C_2 , respectively, for the THISS-2 voter-switch. Using the values assigned in section II to the other variables in equation (1), failure rates for the three-out-of-five voter and THISS-2 voter-switch are computed to be 1.27425×10^{-7} failures/hr and 3.5805×10^{-7} failures/hr, respectively.

The results of the numerical analysis of the safety shutdown systems are presented in Figures 11, 12 and 13. Figure 11 is for the fail-to-danger failure probability for the three-out-of-five voter device while Figure 12 is the fail-to-danger failure probability for the THISS-2 voter-switch (in this particular analysis four-out-of-five voter). Figure 13 gives the results for a false scram failure probability for both the three-out-of-five voter and THISS-2 voter-switch.

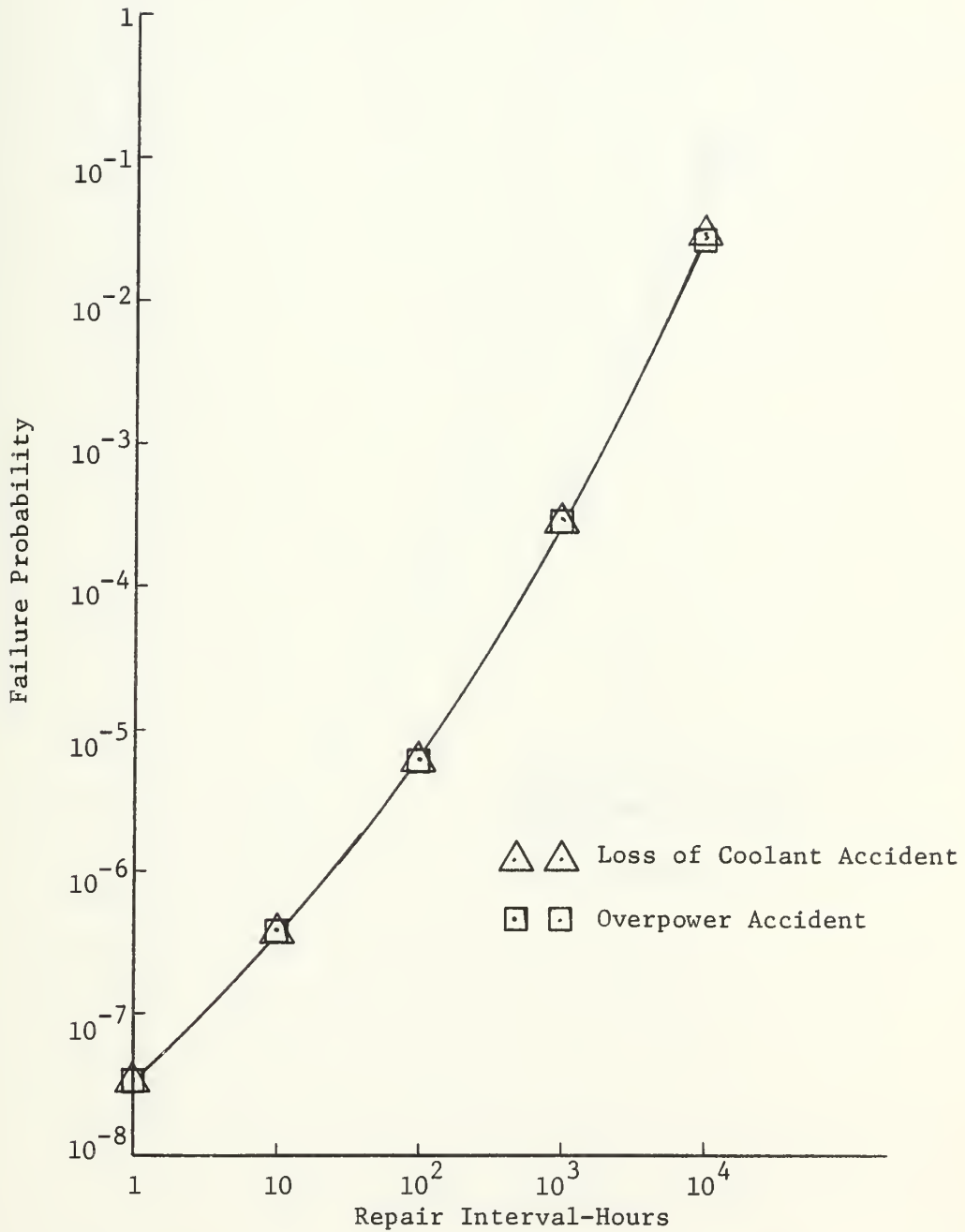


Figure 11. Automatic Safety Shutdown System Failure Probability with Three-out-of-Five Voter Device vs. Repair Time Interval

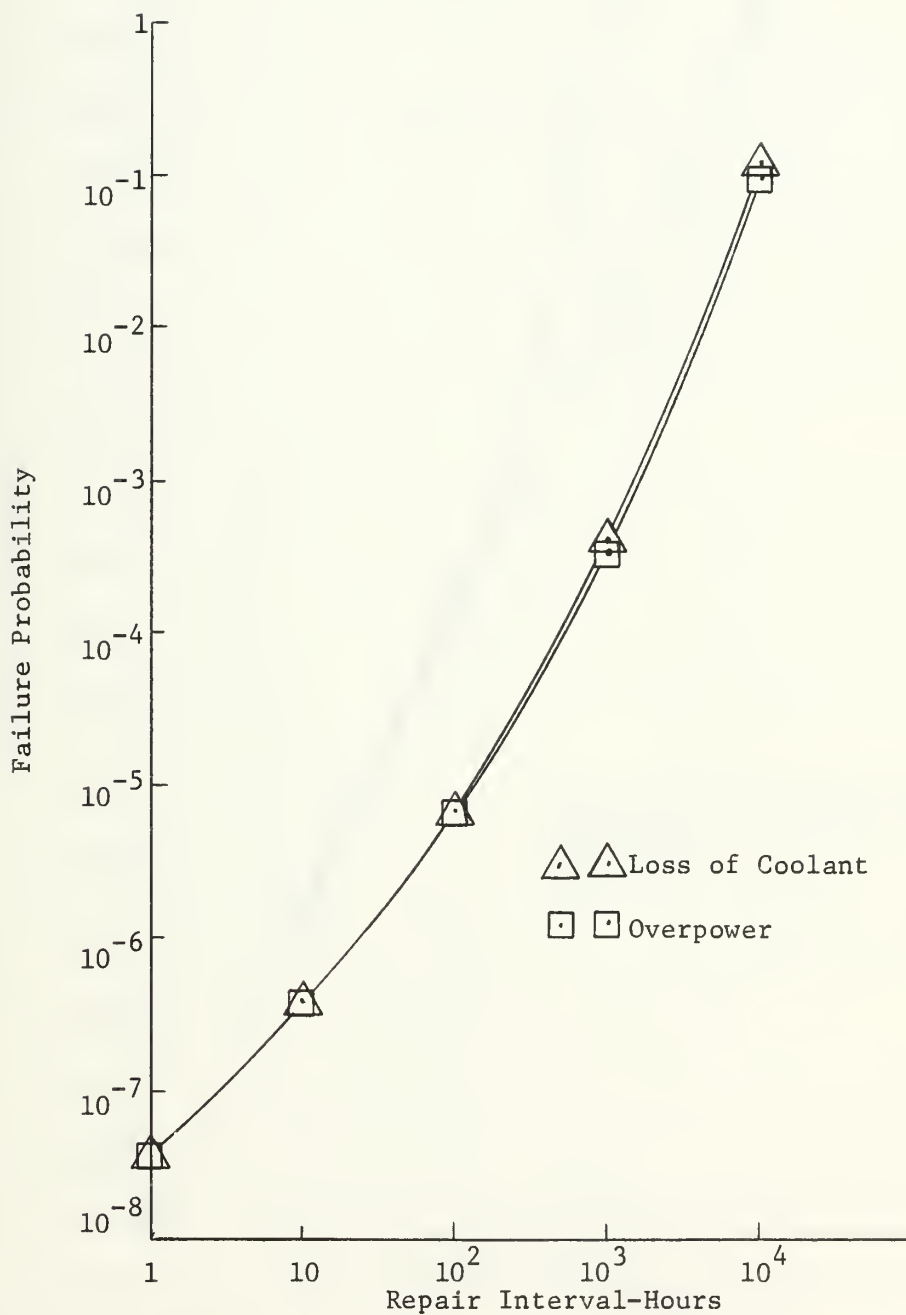


Figure 12: Automatic Safety Shutdown System Failure Probability with THISS-2 Voter-Switch vs. Repair Time Interval

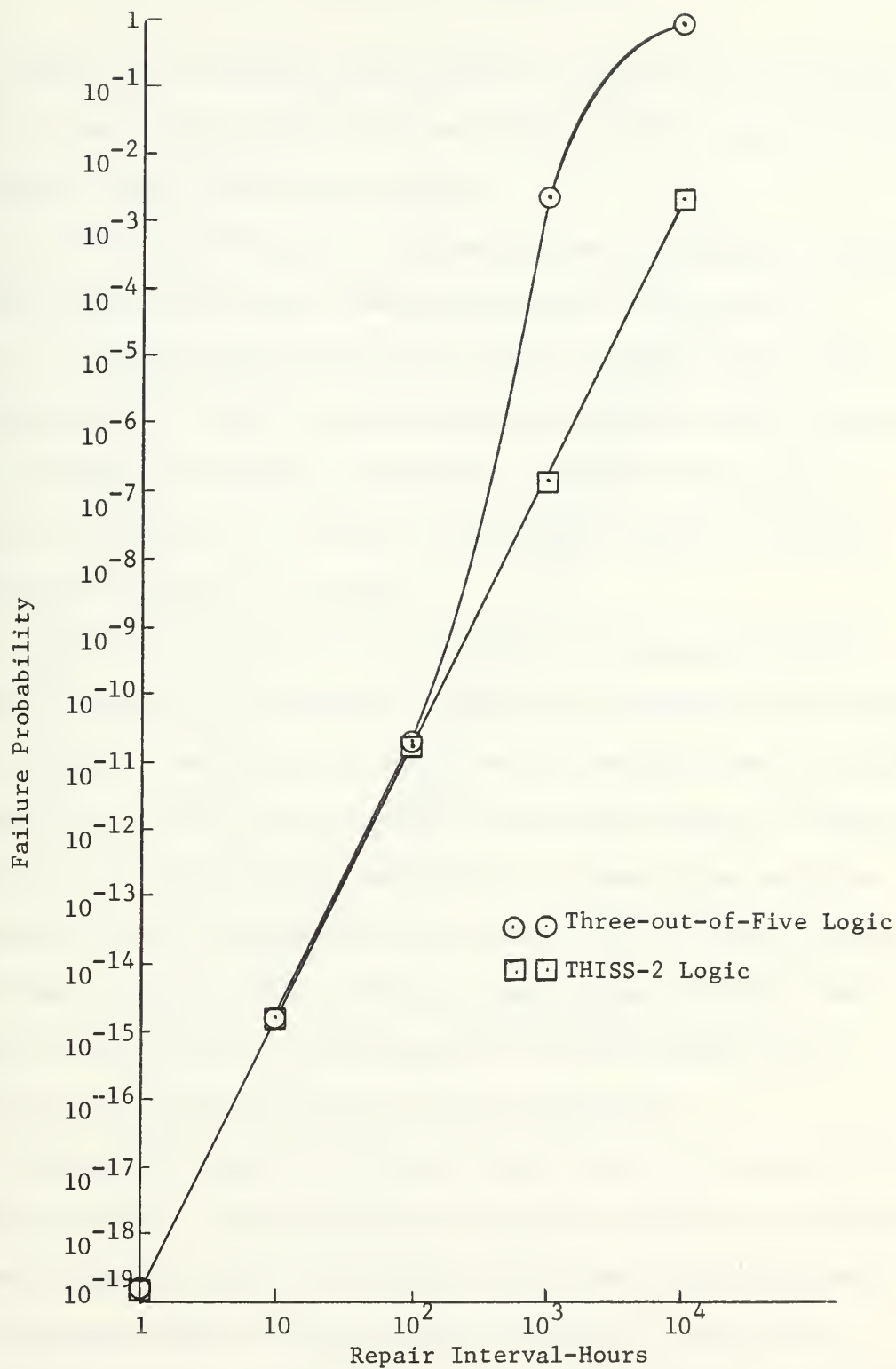


Figure 13. False Scram Failure Probability of Automatic Safety Shutdown Systems vs. Repair Time Interval

VI. SUMMARY AND CONCLUSIONS

Three safety shutdown systems have been analyzed in this study:

1. The original Babcock-241 NSS safety shutdown system utilizing a two-out-of-four channel voter device,
2. A modified Babcock-241 NSS safety system employing a three-out-of-five channel voter device and modified CRDCS trip train, and
3. A second modified form of the Babcock safety system; this system utilizing a THISS-2 voter-switch with modified CRDCS trip train.

For comparison purposes the results presented previously in Figure 4 and Figures 11, 12 and 13 are combined, with the results displayed on Figures 14, 15 and 16.

Figure 14 is the failure probability of the automatic safety shutdown systems for an overpower accident as a function of the repair time interval. The figure indicates that the original two-out-of-four channel voter logic of the Babcock-241 NSS safety system is slightly superior to the two modified systems for all repair time intervals considered. The two modified systems show little difference between each other although at time intervals greater than 10^3 hours, the THISS-2 voter-switch, in this instance a four-out-of-five voter, begins to have a slightly higher failure probability.

Likewise, in Figure 15 the same results exist for the loss of coolant accident. The two-out-of-four channel voter logic system is slightly superior to the two modified systems and little difference exists between these two modified systems except at repair time intervals greater than 10^3 hours. Once again the THISS-2 voter-switch is a four-out-of-five voter.

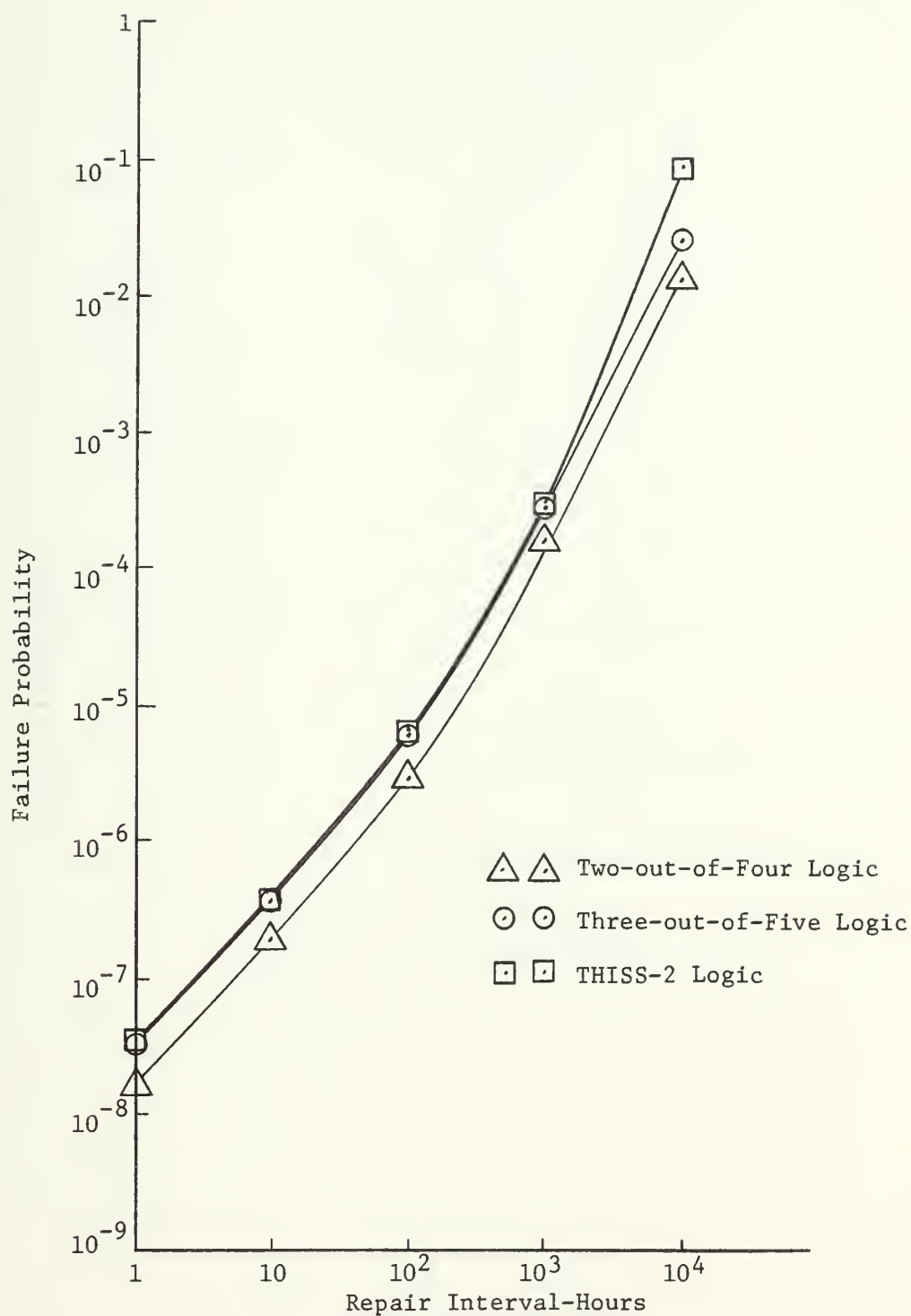


Figure 14. Automatic Safety Shutdown Systems Failure Probability for Overpower Accident vs. Repair Time Interval

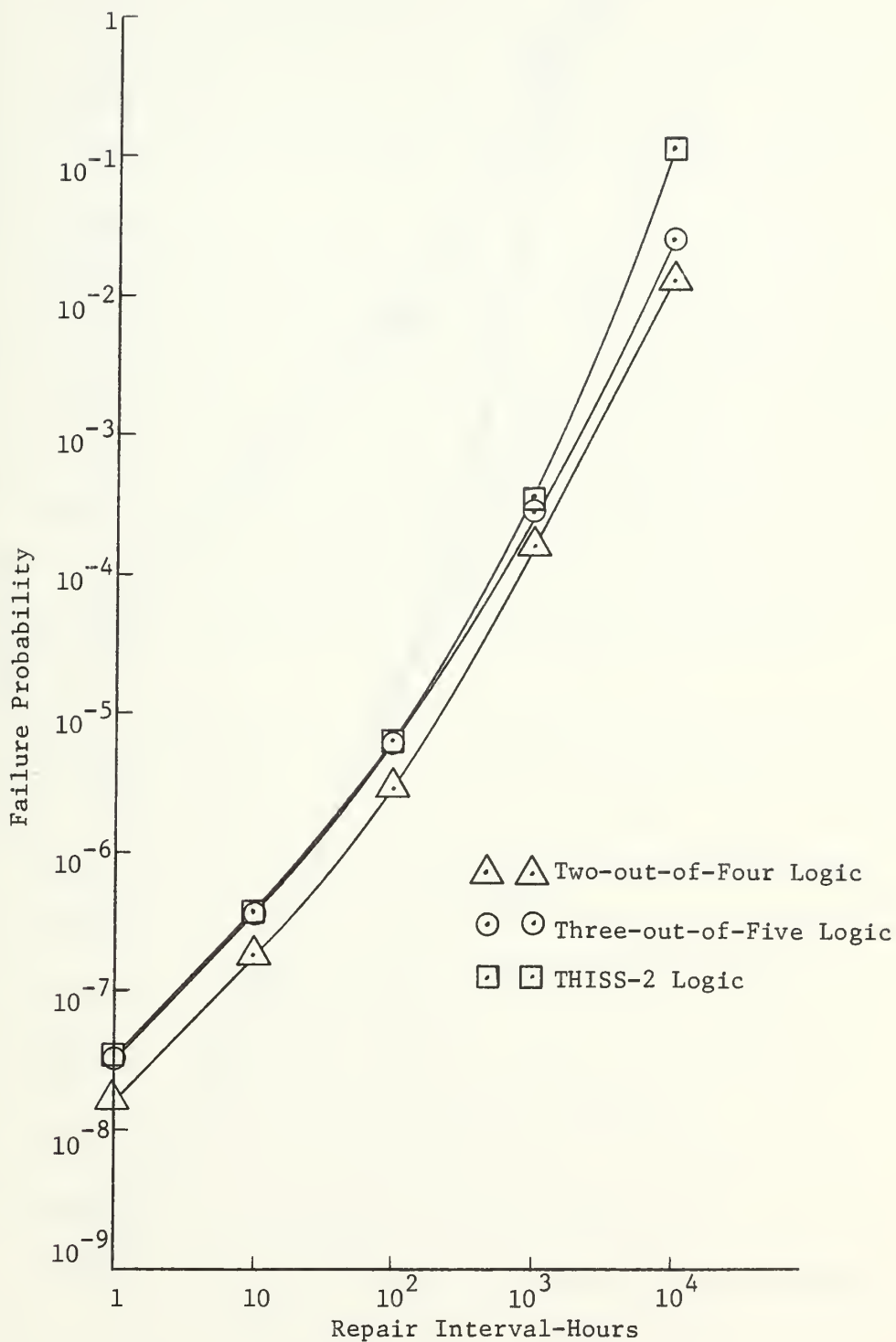


Figure 15. Automatic Safety Shutdown Systems Failure Probability for Loss of Coolant Accident vs. Repair Time Interval

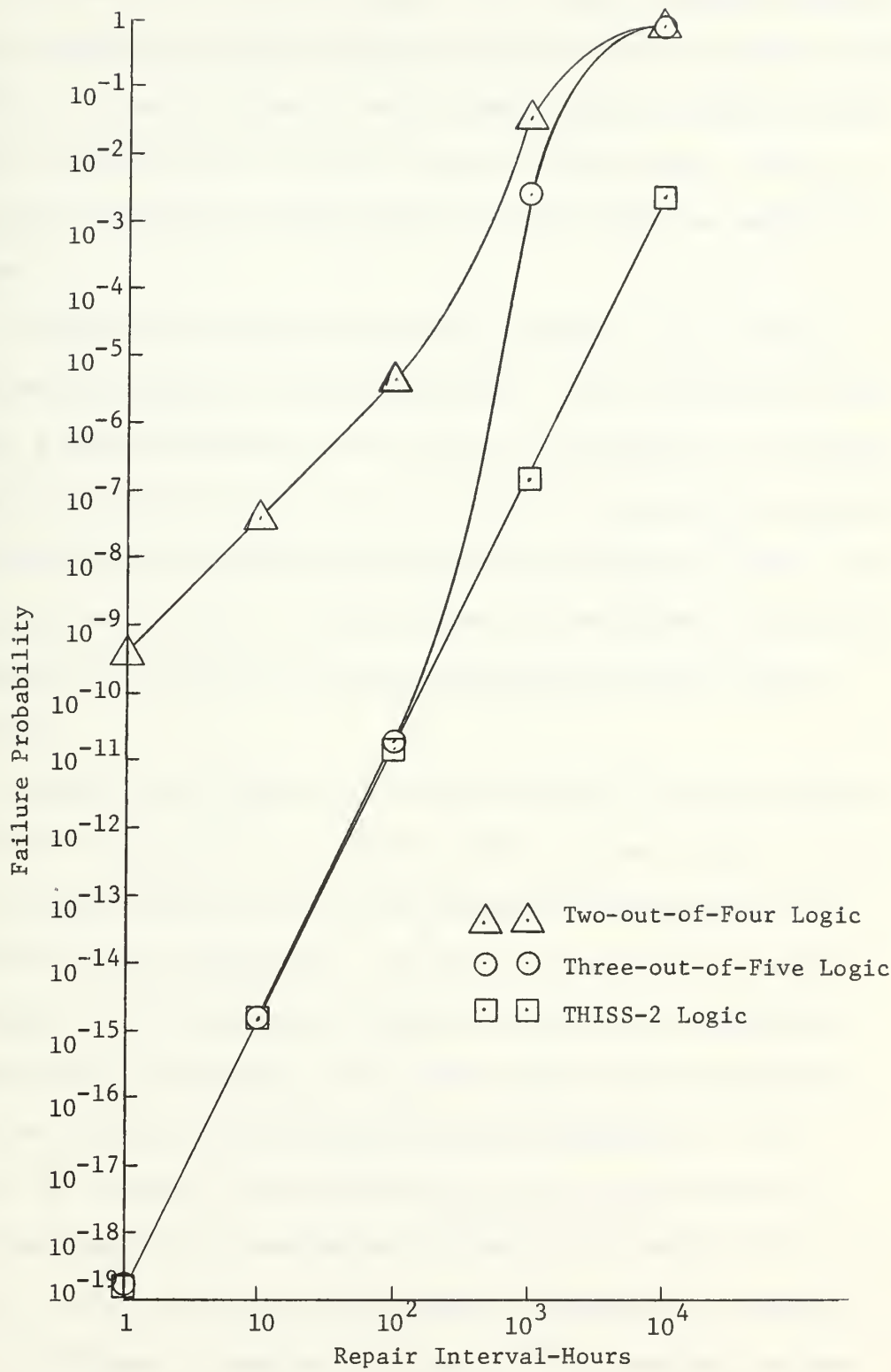


Figure 16. False Scram Failure Probability of Automatic Safety Shutdown Systems vs. Repair Time Interval

Therefore, for a fail-to-danger failure mode, Figures 14 and 15 show no advantage in using computer logic redundancy in safety shutdown circuits. It must be borne in mind, though, that the THISS-2 voter-switch is limited here to being a four-out-of-five voter. This is due to its limitation of being able to tolerate only one undetected failure.

In Figure 16 the advantage of using computer logic redundancy in the safety systems is clearly indicated. As is evident from the figure, a marked decrease in the false scram probability is achieved by using a three-out-of-five voter or THISS-2 voter-switch, especially the voter-switch at repair time intervals approaching 10^4 hours. An improvement on the order of 200 is noted for the THISS-2 voter-switch as compared to the two-out-of-four and three-out-of-five logic at 10^4 hours.

In summary, the THISS-2 voter-switch does and does not offer an advantage in its use in an automatic safety shutdown circuit. For a fail-to-danger failure mode no real advantage is presented for the additional circuit complexity. For the false scram mode a marked improvement in the false scram failure probability is obtainable. In reality this improvement in the false scram failure probability is not an increase in the automatic system reliability. It is, however, an increase in the availability of the reactor which is highly desirable since unwarranted outages are extremely costly to a utility. If the problem with the THISS-2 voter-switch in dealing with its tolerance of undetected failures can be overcome, extreme reliability of the automatic safety shutdown systems, as demanded by

the public, can be achieved along with an increase in the availability of the reactor system desired by the utility.

BIBLIOGRAPHY

1. Schallop, B. Protection System Developments and Trends in the Federal Republic of Germany. Nuclear Safety, Vol. 15, No. 4, p. 409, July-August 1974.
2. Welbourne, D. Computers for Reactor Safety Systems. Nuclear Engineering International, p. 945, November 1974.
3. System 80, Preliminary Safety Analysis Report, CESSAR, Standard Nuclear Steam System Supply, Section 7, Instrumentation and Controls. Combustion Engineering Company, 1974.
4. Babcock 241, Safety Analysis Report. B-SAR-241, Standard Nuclear Steam System, Section 7, Instrumentation and Control. Babcock and Wilcox Company, 1974.
5. Thompson, D., et al. Summary of Abnormal Occurrences Reported to the Atomic Energy Commission During 1973. OOE-OS-001. USAEC Office of Operations Evaluation, May 1974.
6. Avižienis, A., et al. The STAR (Self-Testing and Repairing) Computer: An Investigation of the Theory and Practice of Fault-Tolerant Computer Design. IEEE Transactions on Computers, Vol. C-20, No. 11, p. 1312, November 1971.
7. Washington Public Power Supply System, WPPSS Nuclear Project No. 1, Preliminary Safety Analysis Report, Vol. 4, Sec. 7, October 15, 1973. DOCKET-50460-5.
8. Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. Appendix III-Failure Data. USAEC Report WASH-1400, August 1974.
9. Howard, R. S. A Reliability Analysis of Five Reactor Protection Systems Using a Monte Carlo Technique. M.S. Thesis, The Pennsylvania State University, June 1971.
10. Military Standardization Handbook. Reliability Prediction of Electronic Equipment. MIL-HDBK-217B. Department of Defense, September 1974.
11. ARINC Research Corp. Reliability Engineering. Prentice-Hall, New Jersey, 1964.
12. Shooman, M. L. Probabilistic Reliability: An Engineering Approach. McGraw-Hill, Inc., New York, 1968.
13. Bourne, A. J. and A. E. Green. Reliability Technology. Wiley-Interscience, New York, 1972.

14. Mazzilli, F., et al. RADC Reliability Notebook, Vol. I, Technical Report No. RADC-TR-67-108. (National Technical Information Service No. AD-845304), November 1968.
15. Bazovsky, I. Reliability Theory and Practice. Prentice-Hall, New Jersey, 1961.
16. Taylor, D. S. Reliability and Comparative Analysis of Two Standby System Configurations. IEEE Transactions on Reliability, Vol. R-22, No. 1, p. 13, April 1973.
17. Mathur, F. P. and A. Avižienis. Reliability Analysis and Architecture of a Hybrid-Redundant Digital System: Generalized Triple Modular Redundancy with Self Repair. 1970 Spring Joint Computer Conference. AFIPS Conference Proc., Vol. 36, p. 375, Montvale, New Jersey, AFIPS Press, 1970.
18. Koczella, L. J. A Three-Failure-Tolerant Computer System. IEEE Transactions on Computers, Vol. C-20, p. 1389, November 1971.
19. Ball, M., and F. Hardie. Majority Voter Design Considerations for a TMR Computer. Computer Design, p. 100, April 1969.
20. Brown, W. G., et al. Improvement of Electronic-Computer Reliability Through the Use of Redundancy. IRE Transactions on Electronic Computers, p. 407, September 1961.
21. Mathur, F. P. Reliability Modeling and Analysis of Ultrareliable Fault-Tolerant Digital Systems. IEEE Transactions on Computers, p. 1376, November 1971.
22. Dennis, N. G. Reliability Analysis of Combined Voting and Standby Redundancies. IEEE Transactions on Reliability, Vol. R-23, No. 2, p. 66, June 1974.
23. Goldberg, J. Network Schemes for Combined Fault Masking and Replacement. Working paper presented at the workshop on the organization of reliable automata, Pacific Palisades, California, February 1966. Obtainable from J. Goldberg, Stanford Research Institute, Menlo Park, California, 94025.
24. Dennis, N. G. THISS Voter-Switch Analysis. Proc. Inst. Elec. Eng. (London), Vol. 120, p. 954, September 1973.
25. Bouricius, W. G., et al. Reliability Modeling for Fault-Tolerant Computers. IEEE Trans. Comput., Vol. C-20, p. 1306, November 1971.
26. Mathur, F. P. Reliability Modeling Analysis and Prediction of Ultra-Reliable Fault-Tolerant Digital Systems. 1971 Int. Symp. Digest Fault-Tolerant Computing, p. 79, Computer Society IEEE.

27. Davidow, W. The Rationale of Logic from Semiconductor Memory. 1972 Spring Joint Computer Conference. AFIPS Conference Proceedings, p. 353.
28. Thurber, K. and R. Berg. Universal Logic Modules Implemented Using LSI Memory Techniques. 1971 Fall Joint Computer Conference. AFIPS Conference Proceedings, Vol. 39, p. 177.
29. Lowenschuss, D. Universal LSI Package for Implementing Control Logic Functions. Comp. Design, Vol. 9, p. 67, September 1970.
30. Lapidus, G. Electronic Memories I: Especially Useful as Control Components. Control Eng., Vol. 18, p. 71, October 1971.
31. Peatie, G., et al. Elements of Semiconductor-Device Reliability. Proceedings of IEEE, Vol. 62, p. 149, February 1974.
32. Balfanz, H. P. Failure Rate Compilation. USAEC Report AEC-tr-7564. W. J. Grimes and Company, December 1973.
33. Government-Industry Data Exchange Program. Summaries of Failure Rate Data, Vol. II, Revised, August 1975.

APPENDIX I

Failure Rate Data

Failure rate data used in this study is collected from a variety of sources^{8,9,13,32,33}. The following table lists the failure rates found in the literature and where possible, a range of values is given to indicate the uncertainty of the values.

Table 4
Selected Failure Rate Data

Component	Failure Rate (failures per 10 ⁶ hours)			
	High	Mean	Low	Reference
Amplifiers	146	22	8	33
	37	24	16	33
		20		9
Bridge Completion Unit		20		9
Buffer	22	11	2	33
Calculating Module				
Fails to function		5		*
Shorts		0.5		*
Circuit Breaker				
Premature transfer		1		8
Failure to operate		$1 \times 10^{-3}/D$		8
dP Flow Transmitter		35		32
Ion Chamber		50		9
		5		13
		110 (PWR)		32
		56 (BWR)		32
dP Level Transducer		15		9
		15		32

Table 4 (cont.)

Component	Failure Rate (failures per 10^6 hours)			
	High	Mean	Low	Reference
Line, Gate Driver	43	22	9	33
Logic (Voter) Device		*		*
Power Supply - Instrument		20		9
Vital Bus; Rod Power Supply		0.5		9
Pressure Transducer		15		9
		35		32
Relays				
Open NC contact		0.1		8
Failure NO contacts				
close		0.3		8
Short across NO/NC				
contact		0.01		8
RTD		18.3		32
		40		32
		15		9
		10		13
SCR				
Opens		3		8
Shorts		1		8
Signal Converter	357	53.5	19	33
Square Root Extractor		20		*
Switches				
Manual, fail to transfer		$1 \times 10^{-5}/D$		8
Contacts short		0.1		8
Solid State Devices				
Hi power applications				
Fails to function		3		8
Shorts		1		8
Low power applications				
Fails to function		1		8
Shorts		0.1		8

Table 4 (cont.)

Component	Failure Rate (failures per 10^6 hours)			
	High	Mean	Low	Reference
Transformer				
Open circuit		1		8
Short		1		8

* see Appendix II

APPENDIX II

Failure Rates Used in Analysis

The purpose of this appendix is to assign a failure rate to the various components in this study and justify the value assigned.

Observation of Appendix I indicates a wide range of values existing for some of the components. Data in Appendix I is taken from five sources^{8,9,13,32,33}. No one source is considered more reliable than the others, although more consideration is given to reference 8 due to its origin. Each source is used to complement the others and point out the uncertainty that exists today. It should be noted that references 8, 32 and 33 obtain their data from the same basic sources (FARADA, MIL-HDBK-217A, etc.). In some instances values for particular components could not be located and an intuitive approach is employed in assigning a failure rate. This approach assigns a value for an analogous or similar component or circuit. It is further assumed that since the Babcock and Wilcox design is at the present time a proposal, when a plant is actually built, integrated circuits will be used in a large number of components and thus these components will have lower failure rates than listed in Table 4 in Appendix I. Finally, the value for the voter/voter-switch is computed using the procedure outlined in reference 10.

All types of amplifiers in this study are assigned the same failure rate. The value assigned is 5×10^{-6} failures per hour based on the assumption of integrated circuits being used in their construction.

Bridge completion units are used to convert the signals from the RTD's to current signals. A failure rate of 1×10^{-6} failures per hour is used in this study based on the premise of integrated circuits being used.

Buffers are used to isolate certain portions of the RPS and as such are isolation amplifiers. A value of 5×10^{-6} failures per hour is therefore assigned to this component.

A number of values for circuit breakers can be found (see reference 32 for a listing) in the literature. A value of 1×10^{-6} failures per hour for premature transfer is assigned. Additionally, a value of 1×10^{-3} failures per demand is assigned for failures to operate.

A value of 35×10^{-6} failures per hour is given in reference 32 for a dP flow transmitter. Reference 8 also gives a value for instrumentation but also includes amplification, annunciators, transducers, etc. in the value. It is felt for purposes of this study that to break the system down into greater detail is more advantageous.

A wide range of failure rates for ion chambers is found to exist. A value of 50×10^{-6} failures per hour is arbitrarily assigned to the ion chambers.

References 9 and 32 are in agreement on a value for a dP level transducer. A value of 15×10^{-6} failures per hour is assigned to this component.

Reference 33 gives a median value of 22×10^{-6} failures per hour for a line driver. For purposes of this study however, it is assumed the line driver is composed of integrated circuits and a value of

5×10^{-6} failures per hour is assigned. Additionally, a gate drive is assumed to be similar to a line driver and is assigned the same failure rate.

All types of instrument power supplies are considered to be the same type of device and are arbitrarily assigned a value of 10×10^{-6} failures per hour. The vital bus and rod group power supplies are assigned a value of 0.5×10^{-6} failures per hour.

References 9 and 32 give failure rate values for a pressure transducer. Using these references, a value of 25×10^{-6} failures per hour is assigned.

Three different failure rates are assigned to relays depending upon the failure mode. A value of 0.1×10^{-6} failures per hour is assigned to a normally closed (NC) contact which opens, a value of 0.3×10^{-6} failures per hour to a normally open (NO) contact which fails to close and a value of 0.01×10^{-6} failures per hour for a short across a NC/NO contact.

References 9, 13 and 32 are in close agreement on a failure rate for an RTD. A value of 15×10^{-6} failures per hour is assigned.

Values of 1×10^{-6} and 3×10^{-6} failures per hour are arbitrarily assigned to a SCR which shorts or opens.

Based upon the data found in reference 2, a value of 20×10^{-6} failures per hour is assigned to the signal converter.

For the purposes of this study, a square root extractor is assumed to be similar to a differential amplifier and is accordingly assigned a value of 5×10^{-6} failures per hour.

Values of 1×10^{-5} failures per demand for a manual switch for a failure to transfer and 0.1×10^{-6} failures per hour for switch

contacts shorting are assigned.

All solid state devices are assumed to be similar for purposes of assigning failure rates. The following failure rates are therefore assigned:

High power application (circuits involving currents of 1 ampere or above and/or voltage - 28 volts and above):

Fails to function: 3×10^{-6} failures per hour

Shorts: 1×10^{-6} failures per hour

Low power application:

Fails to function: 1×10^{-6} failures per hour

Shorts: 0.1×10^{-6} failures per hour.

Considered to be solid state items in this analysis are the bistable elements, the channel trip memory circuit, all photo (optical) isolation devices. The calculating module is also considered to be solid state (low power) but is assumed to be five times as complex as the previously mentioned devices, and therefore has a failure rate five times as great.

Finally, transformers are assigned the value 1×10^{-6} failures per hour for both an open circuit and short failure modes.

APPENDIX III

Truth Tables

A truth table approach is used to determine the logic expressions for the modified reliability diagrams using a three-out-of-five voter and the THISS-2 voter-switch.

The truth table associated with the fail-to-danger failure probability is

<u>A(B)</u>	<u>C(D)</u>	<u>E</u>	<u>T</u>
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

where 0 = false

1 = true.

To warrant a 1 in the T column indicates that the safety system will trip the reactor. Out of eight possible trip combinations, five will trip the reactor. The resulting reliability expression is therefore

$$R_{ACE} = R_A R_C R_E + R_A R_C Q_E + R_A Q_C R_E + Q_A R_C R_E + Q_A R_C Q_E \quad (\text{III-1})$$

A similar expression exists for R_{BDE} . Using the relation $R = 1-Q$ and making note of the fact that $R_E = R_A$ which in turn means $Q_E = Q_A$,

equation (III-1) can be simplified to the failure probability form

$$Q'_A = 1.0 - [(1-Q_A)^2(1-Q_C) + 2Q_A(1-Q_A)(1-Q_C) + Q_C(1-Q_A)^2 + Q_A^2(1-Q_C)] \quad (\text{III-2})$$

Once again, a similar expression exists for Q'_B .

An identical procedure is followed for the false scram failure probability. The truth table for this case

<u>A(B)</u>	<u>C(D)</u>	<u>E</u>	<u>T</u>
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

gives rise to the reliability expression

$$R_{ACE} = Q_A R_C R_E + R_A R_C Q_E + R_A R_C R_E. \quad (\text{III-3})$$

Here, only three combinations out of eight will not result in a false scram. Again using the relation $R=1-Q$ and $R_E=R_A$, equation (III-3) can be rewritten in terms of the failure probability

$$Q''_A = 1.0 - [2Q_A(1-Q_C)(1-Q_A) + (1-Q_A)^2(1-Q_C)]. \quad (\text{III-4})$$

A similar expression exists for Q''_B .

Thesis
U8

Utsch

165004

Computer logic redun-
dancy in nuclear reactor
safety shutdown circuits.

28 JUN 76

DISPLAY

Thesis

U8

Utsch

165004

Computer logic redun-
dancy in nuclear reactor
safety shutdown circuits.

thesU8
Computer logic redundancy in nuclear rea



3 2768 001 88961 1
DUDLEY KNOX LIBRARY